STIC Search Report
EIC 2100

STIC Database Tracking Number: 117401

TO:	From:
Kambiz Zand Location: 4C10 Art Unit : 2132 Monday, March 29, 2004 Case Serial Number: 09/598631	Geoffrey St. Leger Location: EIC 2100 PK2-4B30 Phone: 308-7800 geoffrey.stleger@uspto.gov

Search Notes

Dear Examiner Zand,

Attached please find the results of your search request for application 09/598631. I searched Dialog's foreign patent files, product announcement files and general files.

Please let me know if you have any questions.

Regards,

Geoffrey St. Leger
4B30/308-7800

File 348:EUROPEAN PATENTS 1978-2004/Mar W03
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040325,UT=20040318
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	807649	TRAFFIC OR PACKET? ? OR FRAME? ? OR DATAGRAM? ? OR FLOW? ? OR STREAM? ?
S2	71786	(S1 OR DATA OR INFORMATION)(3N)(MALICIOUS OR HARM??? OR DAMAG??? OR DESTRUCTIVE OR UNWANTED OR UNWELCOME OR UNDESIR? OR HOSTILE OR DANGER??? OR SUSPECT OR SUSPICIOUS OR ANOMAL? OR MALEVOLENT OR IRREGULAR? OR ABNORMAL?) OR ATTACK?
S3	1572	DENIAL(1W)SERVICE OR TEARDROP OR PING(1W)DEATH OR SMURF
S4	26142	IDS OR NIDS OR INTRUSION? ?(3N)DETECT???
S5	9137	QOS OR QUALITY(1W)SERVICE
S6	1471	LOW???(2W)PRIORITY
S7	33	HIGH???(2W)PRIORITY
S8	45	PACKET? ?(10N)S5(10N)S6(10N)S7
S9	3	S2:S4(50N)S8
S10	4	S2:S4(100N)S8
S11	6108	S1(5N)(VALID OR VALIDATED OR VERIFIED OR AUTHENTIC OR AUTHENTICATED OR CONFIRMED OR CERTIFIED)
S12	16	S6(20N)S7(20N)S11

10/3,K/1 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00935341 **Image available**
METHODS AND APPARATUS FOR NETWORK ROUTING DEVICE
PROCEDES ET SYSTEME UTILES POUR DISPOSITIF DE ROUTAGE DE RESEAU
Patent Applicant/Assignee:
GOTHAM NETWORKS INC, 15 Discovery Way, Acton, MA 01720, US, US (Residence), US (Nationality)
Inventor(s):
AGGARWAL Vijay, 25 Langelier Lane, Marlboro, MA 01752, US,
BOLAND Wayne, 169 Nagog Hill Road, Acton, MA 01720, US,
MCKINLEY Brittain, 30 Lost Lake Drive, Groton, MA 01450, US,
BEARDSLEY Alan, 23 Loomis Street, Bedford, MA 01730, US,
FLANDERS John, 10 Hunters Lane, Ashland, MA 01721, US,
Legal Representative:
POWSNER David J (et al) (agent), Nutter, McClennen & Fish LLP, One International Place, Boston, MA 02110-2699, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200269575 A1 20020906 (WO 0269575)
Application: WO 2002US6299 20020228 (PCT/WO US0206299)
Priority Application: US 2001272328 20010228; US 2001272387 20010228; US 2001272407 20010228
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 18592

Fulltext Availability:
Claims

Claim
... a 52 byte payload. The header includes parameters such as priority, port number, and egress ID. The reassembled linked-list of buffers that constitutes a **packet** is enqueued on one of four priority output queues that are emptied one GCell at a time, in a high to **low priority** scheme. The dequeued GCells 46 are sent to the Ingress Buffer (IBUF) 48. Illustrated IBUF 48 forwards GCells 46 from the FMU 44 to the...are enqueued on one of four priority output queues in the FMU Data Memory. These queues are emptied one GCell at a time, in a **high** to **low priority** manner. The Header space in the Data Memory not used during the Reassembly is used to fill the Gotham Header. Flow Memory stores 128K Flow...data fi-orn a Queue Processor. The whole scheduling process will select a specific Queue Processor, one (1) of sixteen (I 6), and a specific **QoS** queue, one (1) of four (4), within the selected Queue Processor. Queue Processors are selected on a round robin scheme. The **QoS** queues are selected on 35 a priority scheme, **QoS** queue zero (0) has the **highest priority** level, and **QoS** queue three (3) has the **lowest priority** level.
I
GS Functions
The Global Scheduler has to calculate the **QoS** and Queue Processor select every 1.60 ns. There are three possible criteria to consider in the selection process:
Terminted traffic available, a queue requires...

10/3,K/2 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

....Image available..

METHOD FOR PREVENTING DENIAL OF SERVICE ATTACKS

PROCEDE PERMETTANT D'EMPECHER DES ATTAQUES INFORMATIQUES DE TYPE ATTAQUES PAR DENI DE SERVICE

Patent Applicant/Assignee:
NETRAKE CORPORATION, Suite 100, 3000 Technology Drive, Plano, TX 75074, US, US (Residence), US (Nationality)
Inventor(s):
MAHER Robert Daniel III, 7401 Gurney Drive, Plano, TX 75024, US,
BENNETT Victor A, 5565 FM 549, Rockwall, TX 75032, US,
Legal Representative:
COX Craig J (agent), Netrake Corporation, Suite 100, 3000 Technology Drive, Plano, TX 75074, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200203084 A1 20020110 (WO 0203084)
Application: WO 2001US19492 20010618 (PCT/WO US0119492)
Priority Application: US 2000598631 20000621
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 8028

Fulltext Availability:
Detailed Description
Claims

Detailed Description

... Accordingly, what is needed is a method of preventing DoS attacks and a network device that can perform that method in order to prevent DoS **attacks** from disrupting entire networks.

DISCLOSURE OF INVENTION

The present invention provides for a method of preventing DoS **attacks** . The method involves scanning the contents ...non-overlapping offsets, and adherence to protocol standards. Data Packets that do not verify may be dropped.

After the contents have been verified, the data **packets** are checked to determine if they are associated with a validated traffic flow. If the data **packet** is associated with a validated traffic flow it is assigned to a **higher priority quality** of **service** for transmission back onto the network. If the data **packet** is not associated with a validated traffic flow it is assigned to a **low priority quality** of **service** queue, such that data **packets** in the low priority quality of service queue can occupy no more that a predetermined maximum of the available network bandwidth when they are transmitted back onto the network.

The present invention also includes a network device for preventing DoS **attacks** . The network device includes a traffic flow scanning engine and a quality of service processor. The traffic flow scanning engine is operable to scan the...

...passed to the quality of service processor.

The quality of service processor uses the conclusion from the traffic flow scanning engine to place the data **packets** in the appropriate quality of service queue. Data **packets** associated with validated traffic flow are placed in **higher priority** queues and transmitted back onto the network according to the protocol for the particular queue. Data **packets** not assigned to a validated traffic flow are placed in **low priority QoS** queue. Data **packets** in the low priority QoS queue

are transmitted onto the network such that they occupy no more than a predetermined maximum of available bandwidth, thereby preventing flood tyPe DoS **attacks** .

The foregoing has outlined, rather broadly, preferred and altemative features of the present invention so that those skilled in the art may better understand the...

·laim
... The method of Claim 5 wherein the validated traffic flows are identified by a state associated with each traffic flow.

7 A method of preventing **denial** of **service attacks** on a data network which includes a plurality of traffic flows each formed by multiple data **packets** having header and payload inforination, the method using a network device comprising a traffic flow scanning engine and a **quality** of **service** processor having a **low priority** queue and **higher priority** queues,
the method comprising:
scanning the header infonnation using the traffic flow scanning engine;
. reordering and reassembling the data **packets** using the traffic flow scanning engine; fl agging data packets that do not reorder or reassemble properly to be dropped;
scanning the payload contents using the traffic flow scanning engine;
detemuning whether the data packets confonn to a set of predetennined requirements;
fiagging data **packets** that do not conforin to be dropped;
checking if the data **packets** are associated with a validated traffic flow;
and
assigning data **packets** to a **higher priority quality** of **service** if the data **packet** is associat(inverted question mark)d with a validated traffic flow and to a **low priority quality** of **service** if the data **packet** is not associated with a validated traffic flow.

8 The network device of Claim. 7 wherein the set of predetermined requirerr.,,ents include packet length...

...method of Claim. 7 wherein the validated traffic flows are identified by a state associated with each traffic flow.

12 A network device for preventing **denial** of **service attacks** on a data network which includes a plurality of traffic flows each formed by multiple data packets having contents including header information and payload information...

10/3,K/3 (Item 3 from file: 349)
File 349:PCT FULLTEXT
4 WIPO/Univentio. All rts. reserv.

Image available
A METHOD AND SYSTEM FOR SUPPORTING THE QUALITY OF SERVICE IN WIRELESS NETWORKS
PROCEDE ET SYSTEME POUR PRENDRE EN CHARGE LA QUALITE DU SERVICE DANS DES RESEAUX SANS FIL
Patent Applicant/Assignee:
NOKIA OY,
MIKKONEN Jouni,
SODERLUND Tom,
ALA-LAURILA Juha,
IMMONEN Jukka,
Inventor(s):
MIKKONEN Jouni,
SODERLUND Tom,
ALA-LAURILA Juha,
IMMONEN Jukka,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200013436 A2 20000309 (WO 0013436)
Application: WO 99EP7718 19990827 (PCT/WO EP9907718)
Priority Application: GB 9818873 19980828; GB 9819175 19980901
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK
EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM
TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG
KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF
BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 20504

Fulltext Availability:
Detailed Description

Detailed Description
... which communicate peer-to-peer over the wireless
to link. WFMP actually provides the convergence layer functionality. The
M
Router WFIVIP detects flows, allocates RAN
IDs and informs mobile terminal
WFMP of the assigned ID value. To minimise the overhead the RAN
ID may
be compressed into a shorter radio flow...

...scheduling
queues with different service characteristics, which improves the
wireless support for broadband services. The radio sub-system handles
various radio queues i.e. radio **QoS** classes differently. It may have,
for example, three separate buffering queues for the incoming traffic:
high **priority** queue for realtime traffic, medium priority queue for
non-realtime data and **low** **priority**
queue for best-effort data. Two alternative mechanisms may be used for
mapping the **QoS** requirements of the IP **packets** into the radio level
QoS
functions: direct QoS Mapping or radio flow based QoS mapping of the IP
packets.

Direct QoS Mapping
In the direct...

10/3,K/4 **(Item 4 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00227421
DEVICE AND METHOD FOR IMPLEMENTING QUEUEING DISCIPLINES AT HIGH SSPEEDS
DISPOSITIF ET PROCEDE DE MISE EN OEUVRE DE GESTION DE MISE EN FILE D'ATTENTE A DES VITESSES ELEVEES
Patent Applicant/Assignee:
CODEX CORPORATION,
Inventor(s):
HLUCHYJ Michael G,
BHARGAVA Amit,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9301670 A1 19930121
Application: WO 92US4563 19920601 (PCT/WO US9204563)
Priority Application: US 9165 19910705
Designated States: AU CA JP AT BE CH DE DK ES FR GB GR IT LU MC NL SE
Publication Language: English
Fulltext Word Count: 9428

Fulltext Availability:
Detailed Description

Detailed Description
... does not solve the problem

of data and speech queues affecting the quality of service of each other and of continuous bit-rate data fast **packets** under overload conditions. In HOLP, where speech fast **packets** are given a **high priority**, speech fast **packets** may affect the **quality** of **service** of **lower priority** queues.

Movable boundary schemes for multiplexing speech and data traffic classes of fast **packets** often have **undesirable** delay jitter and underutilize bandwidth allocated to queues having no traffic.

12/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01646215
Method and unit for bit stream decoding
Verfahren und Einheit zur Bitstromdekodierung
Procede et unite pour decoder un flux binaire
PATENT ASSIGNEE:
ROBERT BOSCH GmbH, (200071), Wernerstrasse 1, 70442 Stuttgart, (DE), (Applicant designated States: all)
Daimler Chrysler AG, (3889030), Epplestrasse 225, 70567 Stuttgart, (DE), (Applicant designated States: all)
Bayerische Motoren Werke Aktiengesellschaft, (3259450), Petuelring 130, 80788 Munchen, (DE), (Applicant designated States: all)
Philips Intellectual Property & Standards GmbH, (4300260), Steindamm 94, 20099 Hamburg, DE\(Applicant designated states: , DE)
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (Applicant designated States: all)
General Motors Corporation, (203119), 30200 Mound Road, Warren, MI 48090-9010, (US), (Applicant designated States: all)
Koninklijke Philips Electronics N.V., (200769), Groenewoudseweg 1, 5621 BA Eindhoven, NL\(Applicant designated states: , AT; BE; BG; CH; CY; CZ; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR)
INVENTOR:
Forest, Thomas M., 54503 Berryfield, Macomb, MI 48042-2243, (US)
Hedenetz, Bernd, Bismarckstrasse 40, 73770 Denkendorf, (DE)
Rausch, Mathias, Wallbergstrasse 30, 85570 Marktschwaben, (DE)
Temple, Christopher, Eigerstrasse 29, 81825 Munchen, (DE)
Eisele, Harald, Ulmenallee 12, 25421 Pinneberg, (DE)
Elend, Bernd, Alsterdorfer Strasse 81, 22299 Hamburg, (DE)
Ungermann, Jorn, Am Weissenberg 6, 52074 Aachen, (DE)
Kuhlewein, Matthias, Panoramastrasse 29, 72070 Tubingen, (DE)
Belschner, Ralf, Rigistrasse 10, 72124 Pliezhausen, (DE)
Lohrmann, Peter, Blumhardstrasse 10/1, 73054 Eislingen, (DE)
Bogenberger, Florian, Ingeborgstrasse 3a, 81825 Munchen, (DE)
Wuerz, Thomas, Mitterfeldring 2, 85586 Poing, (DE)
Millsap, Arnold, 2383 Curtis Rd., Leonard, MI 48367, (US)
Heuts, Patrick, De Garf 15, 6581 SJ Malden, (NL)
Hugel, Robert, Joseph-von-Eichendorff-Strasse 9, 76199 Karlsruhe, (DE)
Fuhrer, Thomas, Pappelweg 6, 70839 Gerlingen, (DE)
Muller, Bernd, Eugen-Hegele-Weg 19, 71229 Leonberg, (DE)
Hartwich, Florian, Lerchenstrasse 17/1, 72762 Reutlingen, (DE)
Zinke, Manfred, Altdorfer Strasse 29, 52066 Aachen, (DE)
Berwanger, Josef, Parkweg 1, 85586 Poing, (DE)
Ebner, Christian, Karl-Schmolz-Strasse 21, 80997 Munchen, (DE)
Weiler, Harald, Ziegelstrasse 23/2, 73033 Goppingen, (DE)
Fuhrmann, Peter, Jean-Bremen-Strasse 10, 52080 Aachen, (DE)
Schedl, Anton, Krumbacher Strasse 8, 80798 Munchen, (DE)
Peller, Martin, Bauerstrasse 31, 80796 Munchen, (DE)
LEGAL REPRESENTATIVE:
Dreiss, Fuhlendorf, Steimle & Becker (100863), Patentanwalte Postfach 10 37 62, 70032 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1355461 A2 031022 (Basic)
APPLICATION (CC, No, Date): EP 2003008741 030416;
PRIORITY (CC, No, Date): EP 20028171 020416; DE 10216984 020416
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-012/64
ABSTRACT WORD COUNT: 118
NOTE:
Figure number on first page: 33

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count

CLAIMS A	(English)	200343	541
SPEC A	(English)	200343	70899
Total word count - document A			71440
Total word count - document B			0
Total word count - documents A + B			71440

12/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01646214

Method for monitoring a communication media access schedule of a communication controller of a communication system

Verfahren zur Uberwachung einer Zugriffsablaufsteuerung fur ein Kommunikationsmedium einer Kommunikationssteuerung eines Kommunikations systems

Procede pour surveiller l' acces aux media de communication d' un controleur de communication dans un syteme de communication

PATENT ASSIGNEE:
ROBERT BOSCH GmbH, (200071), Wernerstrasse 1, 70442 Stuttgart, (DE), (Applicant designated States: all)
DaimlerChrysler AG, (3889030), Epplestrasse 225, 70567 Stuttgart, (DE), (Applicant designated States: all)
Bayerische Motoren Werke Aktiengesellschaft, (3259450), Petuelring 130, 80788 Munchen, (DE), (Applicant designated States: all)
Philips Intellectual Property & Standards GmbH, (4300260), Steindamm 94, 20099 Hamburg, DE\(Applicant designated states: , DE)
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (Applicant designated States: all)
General Motors Corporation, (203119), 30200 Mound Road, Warren, MI 48090-9010, (US), (Applicant designated States: all)
Koninklijke Philips Electronics N.V., (200769), Groenewoudseweg 1, 5621 BA Eindhoven, NL\(Applicant designated states: , AT; BE; BG; CH; CY; CZ; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR)

INVENTOR:
Forest, Thomas M., 54503 Berryfield, Macomb, MI 48042-2243, (US)
Hedenetz, Bernd, Bismarckstrasse 40, 73770 Denkendorf, (DE)
Rausch, Mathias, Wallbergstrasse 30, 85570 Marktschwaben, (DE)
Temple, Christopher, Eigerstrasse 29, 81825 Munchen, (DE)
Eisele, Harald, Ulmenallee 12, 25421 Pinneberg, (DE)
Elend, Bernd, Alsterdorfer Strasse 81, 22299 Hamburg, (DE)
Ungermann, Jorn, Am Weisenberg 6, 52074 Aachen, (DE)
Kuhlewein, Matthias, Panoramastrasse 29, 72070 Tubingen, (DE)
Belschner, Ralf, Rigistrasse 10, 72124 Pliezhausen, (DE)
Lohrmann, Peter, Blumhardstrasse 10/1, 73054 Eislingen, (DE)
[illegible]berger, Florian, Ingeborgstrasse 3a, 81825 Munchen, (DE)
[illegible], Thomas, Mitterfeldring 2, 85586 Poing, (DE)
[illegible], Arnold, 2383 Curtis Rd., Leonard, MI 48367, (US)
[illegible], Patrick, De Garf 15, 6581 SJ Malden, (NL)
Engel, Robert, Joseph-von-Eichendorff-Strasse 9, 76199 Karlsruhe, (DE)
Fuhrer, Thomas, Pappelweg 6, 70839 Gerlingen, (DE)
Muller, Bernd, Eugen-Hegele-Weg 19, 71229 Leonberg, (DE)
Hartwich, Florian, Lerchenstrasse 17/1, 72762 Reutlingen, (DE)
Zinke, Manfred, Altdorfer Strasse 29, 52066 Aachen, (DE)
Berwanger, Josef, Parkweg 1, 85586 Poing, (DE)
Ebner, Christian, Karl-Schmolz-Strasse 21, 80997 Munchen, (DE)
Weiler, Harald, Ziegelstrasse 23/2, 73033 Goppingen, (DE)
Fuhrmann, Peter, Jean-Bremen-Strasse 10, 52080 Aachen, (DE)
Schedl, Anton, Krumbacher Strasse 8, 80798 Munchen, (DE)
Feller, Martin, Bauerstrasse 31, 80796 Munchen, (DE)

LEGAL REPRESENTATIVE:
Dreiss, Fuhlendorf, Steimle & Becker (100863), Patentanwalte Postfach 10 37 62, 70032 Stuttgart, (DE)

PATENT (CC, No, Kind, Date): EP 1355460 A2 031022 (Basic)
APPLICATION (CC, No, Date): EP 2003008740 030416;
PRIORITY (CC, No, Date): EP 20028171 020416; DE 10216984 020416

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-012/64
ABSTRACT WORD COUNT: 180
NOTE:
Figure number on first page: 119
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200343	1216
SPEC A	(English)	200343	74486
Total word count - document A			75702
Total word count - document B			0
Total word count - documents A + B			75702

12/3,K/3 **(Item 3 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01646213
Method for synchronizing clocks in a distributed communication system
Verfahren zum Synchronisieren von Uhren in einem verteilten Kommunikationssystem
Procede pour synchroniser des horologes dans un systeme de communication distribue
PATENT ASSIGNEE:
ROBERT BOSCH GmbH, (200071), Wernerstrasse 1, 70442 Stuttgart, (DE), (Applicant designated States: all)
Daimler Chrysler AG, (3889030), Epplestrasse 225, 70567 Stuttgart, (DE), (Applicant designated States: all)
Bayerische Motoren Werke Aktiengesellschaft, (3259450), Petuelring 130, 80788 Munchen, (DE), (Applicant designated States: all)
Philips Intellectual Property & Standards GmbH, (4300260), Steindamm 94, 20099 Hamburg, DE\(Applicant designated states: , DE)
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (Applicant designated States: all)
General Motors Corporation, (203119), 30200 Mound Road, Warren, MI 48090-9010, (US), (Applicant designated States: all)
Koninklijke Philips Electronics N.V., (200769), Groenewoudseweg 1, 5621 BA Eindhoven, NL\(Applicant designated states: , AT; BE; BG; CH; CY; CZ; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LU; MC; NL; PT; SE; SI; SK; TR; RO)
INVENTOR:
Preuss, Thomas M., 54503 Berryfield, Macomb, MI 48042-2243, (US)
Hedenetz, Bernd, Bismarckstrasse 40, 73770 Denkendorf, (DE)
Rausch, Mathias, Wallbergstrasse 30, 85570 Marktschwaben, (DE)
Temple, Christopher, Eigerstrasse 29, 81825 Munchen, (DE)
Eisele, Harald, Ulmenallee 12, 25421 Pinneberg, (DE)
Elend, Bernd, Alsterdorfer Strasse 81, 22299 Hamburg, (DE)
Ungermann, Jorn, Am Weisenberg 6, 52074 Aachen, (DE)
Kuhlewein, Matthias, Panoramastrasse 29, 72070 Tubingen, (DE)
Belschner, Ralf, Rigistrasse 10, 72124 Pliezhausen, (DE)
Lohrmann, Peter, Blumhardstrasse 10/1, 73054 Eislingen, (DE)
Bogenberger, Florian, Ingeborgstrasse 3a, 81825 Munchen, (DE)
Wuerz, Thomas, Mitterfeldring 2, 85586 Poing, (DE)
Millsap, Arnold, 2383 Curtis Rd., Leonard, MI 48367, (US)
Peeters, Patrick, De Garf 15, 6581 SJ Malden, (NL)
Bogel, Robert, Joseph-von-Eichendorff-Strasse 9, 76199 Karlsruhe, (DE)
Fuhrer, Thomas, Pappelweg 6, 70839 Gerlingen, (DE)
Muller, Bernd, Eugen-Hegele-Weg 19, 71229 Leonberg, (DE)
Hartwich, Florian, Lerchenstrasse 17/1, 72762 Reutlingen, (DE)
Zinke, Manfred, Altdorfer Strasse 29, 52066 Aachen, (DE)
Berwanger, Josef, Parkweg 1, 85586 Poing, (DE)
Ebner, Christian, Karl-Schmolz-Strasse 21, 80997 Munchen, (DE)
Weiler, Harald, Ziegelstrasse 23/2, 73033 Goppingen, (DE)
Fuhrmann, Peter, Jean-Bremen-Strasse 10, 52080 Aachen, (DE)

Pfeiffer, Anton, Krumbacher Strasse 8, 80798 Munchen, (DE)
Peller, Martin, Bauerstrasse 31, 80796 Munchen, (DE)
LEGAL REPRESENTATIVE:
Dreiss, Fuhlendorf, Steimle & Becker (100863), Patentanwalte Postfach 10 37 62, 70032 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1355459 A2 031022 (Basic)
APPLICATION (CC, No, Date): EP 2003008739 030416;
PRIORITY (CC, No, Date): EP 20028171 020416; DE 10216984 020416
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-012/64
ABSTRACT WORD COUNT: 89
NOTE:
Figure number on first page: 44

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200343	758
SPEC A	(English)	200343	72113
Total word count - document A			72871
Total word count - document B			0
Total word count - documents A + B			72871

12/3,K/4 **(Item 4 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01646211
Method for transmitting data within a communication system
Verfahren zur Datenubertragung in einem Kommunikatinsystem
Procede pour la transmission de donnees dans un systeme de communication
PATENT ASSIGNEE:
ROBERT BOSCH GmbH, (200071), Wernerstrasse 1, 70442 Stuttgart, (DE), (Applicant designated States: all)
Daimler Chrysler AG, (3889030), Epplestrasse 225, 70567 Stuttgart, (DE), (Applicant designated States: all)
Bayerische Motoren Werke Aktiengesellschaft, (3259450), Petuelring 130, 80788 Munchen, (DE), (Applicant designated States: all)
Philips Intellectual Property & Standards GmbH, (4300260), Steindamm 94, 20099 Hamburg, DE\(Applicant designated states: , DE)
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (Applicant designated States: all)
General Motors Corporation, (203119), 30200 Mound Road, Warren, MI 48090-9010, (US), (Applicant designated States: all)
Koninklijke Philips Electronics N.V., (200769), Groenewoudseweg 1, 5621 BA Eindhoven, NL\(Applicant designated states: , AT; BE; BG; CH; CY; CZ; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR)
INVENTOR:
Forest, Thomas M., 54503 Berryfield, Macomb, MI 48042-2243, (US)
Rademacher, Bernd, Bismarckstrasse 40, 73770 Denkendorf, (DE)
Rausch, Mathias, Wallbergstrasse 30, 85570 Marktschwaben, (DE)
Temple, Christopher, Eigerstrasse 29, 81825 Munchen, (DE)
Eisele, Harald, Ulmenallee 12, 25421 Pinneberg, (DE)
Elend, Bernd, Alsterdorfer Strasse 81, 22299 Hamburg, (DE)
Ungermann, Jorn, Am Weisenberg 6, 52074 Aachen, (DE)
Kuhlewein, Matthias, Panoramastrasse 29, 72070 Tubingen, (DE)
Belschner, Ralf, Rigistrasse 10, 72124 Pliezhausen, (DE)
Lohrmann, Peter, Blumhardstrasse 10/1, 73054 Eislingen, (DE)
Bogenberger, Florian, Ingeborgstrasse 3a, 81825 Munchen, (DE)
Wuerz, Thomas, Mitterfeldring 2, 85586 Poing, (DE)
Millsap, Arnold, 2383 Curtis Rd., Leonard, MI 48367, (US)
Heuts, Patrick, De Garf 15, 6581 SJ Malden, (NL)
Hugel, Robert, Joseph-von-Eichendorff-Strasse 9, 76199 Karlsruhe, (DE)
Fuhrer, Thomas, Pappelweg 6, 70839 Gerlingen, (DE)

Muller, Bernd, Eugen-Hegele-Weg 19, 71229 Leonberg, (DE)
Hartwich, Florian, Lerchenstrasse 17/1, 72762 Reutlingen, (DE)
Zinke, Manfred, Altdorfer Strasse 29, 52066 Aachen, (DE)
Berwanger, Josef, Parkweg 1, 85586 Poing, (DE)
Feiner, Christian, Karl-Schmolz-Strasse 21, 80997 Munchen, (DE)
Weiler, Harald, Ziegelstrasse 23/2, 73033 Goppingen, (DE)
Fuhrmann, Peter, Jean-Bremen-Strasse 10, 52080 Aachen, (DE)
Schedl, Anton, Krumbacher Strasse 8, 80798 Munchen, (DE)
Peller, Martin, Bauerstrasse 31, 80796 Munchen, (DE)
LEGAL REPRESENTATIVE:
Dreiss, Fuhlendorf, Steimle & Becker (100863), Patentanwalte Postfach 10 37 62, 70032 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 1355458 A2 031022 (Basic)
APPLICATION (CC, No, Date): EP 2003008737 030416;
PRIORITY (CC, No, Date): EP 20028171 020416; DE 10216984 020416
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04L-012/64
ABSTRACT WORD COUNT: 122
NOTE:
Figure number on first page: 95

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200343	830
SPEC A	(English)	200343	71844
Total word count - document A			72674
Total word count - document B			0
Total word count - documents A + B			72674

12/3,K/5 **(Item 5 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01379961
Methods and devices of allocating slots to child stations
Verfahren und Vorrichtungen zur Zuweisung von Schlitzen an Unterstationen
Methodes et dispositifs d'allocation de creneaux aux stations subordonnees
PATENT ASSIGNEE:
MITSUBISHI DENKI KABUSHIKI KAISHA, (208589), 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP), (Applicant designated States: all)
INVENTOR:
Arita, Minoru, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
Asashiba, Yoshihiro, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
Suzuki, Takamasa, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
LEGAL REPRESENTATIVE:
Bohnenberger, Johannes, Dr. et al (55291), Meissner, Bolte & Partner Postfach 86 06 24, 81633 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1172955 A2 020116 (Basic)
APPLICATION (CC, No, Date): EP 2001116345 010705;
PRIORITY (CC, No, Date): JP 2000214923 000714; JP 20013465 010111; JP 200145530 010221
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04J-003/16; H04B-010/207
ABSTRACT WORD COUNT: 224
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200203	5018
SPEC A	(English)	200203	31106
Total word count - document A			36124
Total word count - document B			0
Total word count - documents A + B			36124

...SPECIFICATION and 60c, 75 indicates a communication traffic informing packet producing unit for producing a type of communication traffic informing packet having information of a communication **traffic** of **valid** information **packets** sent from the child station device. The **high priority** packets produced in the **high priority** packet producing unit 62, the low priority operation and maintenance packets produced in the **low priority** operation and maintenance packet producing units 64 and the upward information **packets** are included in the **valid** information **packets** .

76 indicates a **packet** multiplexing unit for multiplexing the communication traffic informing packet produced in the communication traffic informing packet producing unit 75 with the **high priority** packet produced in the **high priority** packet producing unit 62.

77 indicates a high priority buffer for storing the communication traffic informing packet and the high priority packet multiplexed with each...

12/3,K/6 (Item 6 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01321871

Transmission of high-priority, real-time traffic on low-speed communications links

Verfahren zur Ubertragung von hochprioritats Echtzeitdatenverkehr uber niedriggeschwindigkeits Kommunikationsverbindungen

Procede pour la transmission de trafic a haute priorite en temps reel sur des liens de communication a faible debit

PATENT ASSIGNEE:
INTERNATIONAL BUSINESS MACHINES CORPORATION, (200123), , Armonk, NY 10504, (US), (Applicant designated States: all)

INVENTOR:
Cidon, Israel, Technion-I.I.T., Haifa 32000, (IL)
Drake, John Ellis Jr., 70854 S. Normal, Chicago, IL 60628, (US)
Potter, Kenneth Harvey Jr., 5404 Amsterdam Place, Raleigh, NC 27606-9708, (US)
Doney, Richard M., 7 Banneret Place, Durham, NC 27713, (US)
Hervatic, Elizabeth Anne, 4908 Matlock St., Apex, NC 27502, (US)
Tedijanto, Theodore Ernest, 2011 Trenton Court, Cranberry Township, PA 16066, (US)

LEGAL REPRESENTATIVE:
Etorre, Yves Nicolas (87833), Compagnie IBM-France, Direction de la Propriete Intellectuelle, 06610 La Gaude, (FR)

PATENT (CC, No, Kind, Date): EP 1128612 A2 010829 (Basic)
APPLICATION (CC, No, Date): EP 2001108461 930716;
PRIORITY (CC, No, Date): US 927697 920807
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IT; LI; NL; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 582537 (EP 93480096)
INTERNATIONAL PATENT CLASS: H04L-012/56
ABSTRACT WORD COUNT: 110
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	357
SPEC A	(English)	200135	4466
Total word count - document A			4823

Total word count - document B 0
Total word count - documents A + B 4823

...SPECIFICATION a basic packet frame used in the practice of this invention, where packet containing header and data is delimited by flags;

Figure 2 shows the **valid** combination of formatted **packet frames** in which a **low - priority** packet is preempted by a **high - priority** packet with subsequent automatic resumption;
Figure 3 shows a combination of packet frames containing a bit error which causes a transmission abort;
Figure 4 shows...of packets and flags when preempt/resume is not enabled.

7E ((7E) (RTP 7E) (7E) (NRTP 7E))
Under the foregoing rules, the following is a **valid** combination of **packets** and flags when preempt/resume is enabled : where
* () denotes optional and repeatable fields
* {} denotes required, repeatable fields
* F represents the bytealigned flag (B'01111110', X'7E')
* RTP represents a **high - priority** packet
* NRTP represents a **low - priority** packet
* (NRTP represents portions of a preempted **low - priority** packet
* SP represents a start-preempt flag (B'011111110')
* EP represents an end-preempt flag (B'0111111110')
Figure 1 shows a conventional frame 10 delimited by normal (starting and ending) 7E flags 10a and containing both a control header 10b field and a data 10c field.
Figure 2 illustrates in **frame** sequence 20 a preempt **valid** operation in more detail with the case of a **low priority** packet being preempted by two consecutive **high - priority** packets. The first field 20a shows the normal bytealigned starting flag X'7E'. The second field 20b is an ongoing **low - priority** packet NRTP1. The third field 20c shows a start-preempt or SP flag bit by bit. This SP flag interrupts the low-priority packet and...

12/3,K/7 **(Item 7 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

00605868
Transmission of high-priority, real-time traffic on low-speed communications links.
Ubertragung von Echtzeitverkehr hoher Prioritat uber langsame Ubertragungsverbindungen.
Transmission de trafic de haute priorite sur lignes de communication a basse vitesse.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;NL;SE)
INVENTOR:
Cidon, Israel, Technion - I.I.T., Haifa 32000, (IL)
Doney, Richard M., 5724 Fortunes Ridge Drive, Durham, NC 27713, (US)
Drake, John Ellis, Jr., 321 Fearrington, Pittsboro, NC 27312, (US)
Hervatic, Elizabeth Anne, 4908 Matlock Street, Apex, NC 27502, (US)
Potter, Kenneth Harvey, Jr., 5404 Amsterdam Place, Raleigh, NC 27606-9708, (US)
Tedijanto, Theodore Ernest, 106 Tasman Court, Cary, NC 27513, (US)
LEGAL REPRESENTATIVE:
de Pena, Alain (15151), Compagnie IBM France Departement de Propriete Intellectuelle, F-06610 La Gaude, (FR)
PATENT (CC, No, Kind, Date): EP 582537 A2 940209 (Basic)
EP 582537 A3 950524
APPLICATION (CC, No, Date): EP 93480096 930716;
PRIORITY (CC, No, Date): US 927697 920807
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IT; LI; NL; SE

RELATED DIVISIONAL NUMBER(S) - PN (AN):
(EP 2001108461)
INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-012/64;
ABSTRACT WORD COUNT: 114

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	706
SPEC A	(English)	EPABF2	4021
Total word count - document A			4727
Total word count - document B			0
Total word count - documents A + B			4727

...SPECIFICATION a basic packet frame used in the practice of this invention, where packet containing header and data is delimited by flags;

Figure 2 shows the **valid** combination of formatted **packet frames** in which a **low - priority** packet is preempted by a **high - priority** packet with subsequent automatic resumption;

Figure 3 shows a combination of packet frames containing a bit error which causes a transmission abort;

Figure 4 shows...following is a valid combination of packets and flags when preempt/resume is not enabled. (Formula omitted)

Under the foregoing rules, the following is a **valid** combination of **packets** and flags when preempt/resume is enabled : (see image in original document)

where

- () denotes optional and repeatable fields
- () denotes required, repeatable fields
- 7E represents the byte-aligned flag (B'01111110', X'7E')
- RTP represents a **high - priority** packet
- NRTP represents a **low - priority** packet
- pNRTP represents portions of a preempted low-priority packet
- SP represents a start-preempt flag (B'011111110')
- EP represents an end-preempt flag (B...

...by normal (starting and ending) 7E flags 10a and containing both a control header 10b field and a data 10c field.

Figure 2 illustrates in **frame** sequence 20 a preempt **valid** operation in more detail with the case of a **low priority** packet being preempted by two consecutive **high - priority** packets. The first field 20a shows the normal byte-aligned starting flag X'7E'. The second field 20b is an ongoing **low - priority** packet NRTP1. The third field 20c shows a start-preempt or SP flag bit by bit. This SP flag interrupts the low-priority packet and...

12/3,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00496224
Method and apparatus for the testing and evaluation of geographically distributed telecommunication networks.
Verfahren und Gerat zur Prufung und Auswertung von geographisch verteilten Fernmeldenetzen.
Methode et appareil pour tester et evaluer des reseaux de telecommunication distribues geographiquement.
PATENT ASSIGNEE:
INTERNATIONAL BUSINESS MACHINES CORPORATION, (200123), , Armonk, NY 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Engbersen, Antonius, Dr., Speerstrasse 63, CH-8805 Richterswil, (CH)
Heddes, Marco, Hornhaldenstrasse 1, CH-8802 Kilchberg, (CH)
Herkersdorf, Andreas, Dr., Lebernstrasse 15, CH-8134 Adliswil, (CH)
Luijten, Ronald, Seestrasse 80, CH-8942 Oberrieden, (CH)
Rothauser, Ernst, Dr., Am Steinenbruggli, CH-8864 Reichenburg, (CH)

LEGAL REPRESENTATIVE:
  Rudack, Gunter O., Dipl.-Ing. (26662), IBM Corporation Saumerstrasse 4, CH-8803 Ruschlikon, (CH)
PATENT (CC, No, Kind, Date): EP 504537 A1 920923 (Basic)
APPLICATION (CC, No, Date): EP 91810203 910322;
PRIORITY (CC, No, Date): EP 91810203 910322
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-012/26;
ABSTRACT WORD COUNT: 237

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1134
SPEC A	(English)	EPABF1	13837
Total word count - document A			14971
Total word count - document B			0
Total word count - documents A + B			14971

...SPECIFICATION length. The data stream from the switching system is accompanied by a packet delimiter which carries a logic low signal during the transmission of a **valid packet** . Length error checker 36 extracts the type bit of an arriving packet (which is used to distinguish between a **high - priority** packet and a 256-bit **low - priority** packet), counts the clock cycles during which the packet delimiter stays low, and determines whether the received packet has a correct length or not. The...

12/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00459834
Methods and apparatus for implementing a media access control/host system interface.
Verfahren und Gerat zur Ausfuhrung einer Mediumzugriffssteuerung/Wirtsystem schnittstelle.
Methode et appareil pour realiser le controle d'acces au media/interface avec le systeme hote.
PATENT ASSIGNEE:
  NATIONAL SEMICONDUCTOR CORPORATION, (262383), 2900 Semiconductor Drive, Santa Clara, CA. 95051-8090, (US), (applicant designated states: BE;DE;FR;GB;IT;LU;NL)
INVENTOR:
  Travaglio, Mark A., 2a Eastern Rd, Scarborough, Maine 04074, (US)
  Young, Desmond W., 231 No. San Tomas Aquino, Campbell, CA 95008, (US)
  Brief, David C., 35 Winslow Rd, Brookline, MA 02146, (US)
  Hamstra, James R., 23930 Yellowstone Trail, Shorewood, MN 55531, (US)
LEGAL REPRESENTATIVE:
  Harding Rohl Henseler Patentanwalte European Patent Attorneys (100362), Bernhardstrasse 123, W-4000 Dusseldorf 1, (DE)
PATENT (CC, No, Kind, Date): EP 453863 A2 911030 (Basic)
EP 453863 A3 940406
APPLICATION (CC, No, Date): EP 91105583 910409;
PRIORITY (CC, No, Date): US 516245 900427
DESIGNATED STATES: BE; DE; FR; GB; IT; LU; NL
INTERNATIONAL PATENT CLASS: H04L-029/06;
ABSTRACT WORD COUNT: 149

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	2022
SPEC A	(English)	EPABF1	28289
Total word count - document A			30311
Total word count - document B			0
Total word count - documents A + B			30311

...SPECIFICATION 1 and **Low - priority** async frames onto ISAP...

...2. The most significant bit of the three-bit priority field determines **High / Low priority** .
The ISAPs each write indicate data to separate memory pages and each has its own PSP Queue. This allows a variety of pool space management...

12/3,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

0106062
Digital data processing system.
Digitales Datenverarbeitungssystem.
Systeme du traitement de donnees numeriques.
PATENT ASSIGNEE:
DATA GENERAL CORPORATION, (410940), Route 9, Westboro Massachusetts 01581, (US), (applicant designated states: AT;BE;CH;DE;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
Bratt, Richard Glenn, 9 Brook Trail Road, Wayland Massachusetts 01778, (US)
Clancy, Gerald F., 13069 Jaccaranda Center, Saratoga California 95070, (US)
Gavrin, Edward S., Beaver Pond Road RFD 4, Lincoln Massachusetts 01773, (US)
Gruner, Ronald Hans, 112 Dublin Wood Drive, Cary North Carolina 27514, (US)
Mundie, Craig James, 136 Castlewood Drive, Cary North Carolina, (US)
Schleimer, Stephen I., 1208 Ellen Place, Chapel Hill North Carolina 27514, (US)
Wallach, Steven J., 12436 Green Meadow Lane, Saratoga California 95070, (US)
LEGAL REPRESENTATIVE:
Robson, Aidan John et al (69471), Reddie & Grose 16 Theobalds Road, London WC1X 8PL, (GB)
PATENT (CC, No, Kind, Date): EP 300516 A2 890125 (Basic)
EP 300516 A3 890426
EP 300516 B1 931124
APPLICATION (CC, No, Date): EP 88200921 820521;
PRIORITY (CC, No, Date): US 266413 810522; US 266539 810522; US 266521 810522; US 266415 810522; US 266409 810522; US 266424 810522; US 266421 810522; US 266404 810522; US 266414 810522; US 266532 810522; US 266403 810522; US 266408 810522; US 266401 810522; US 266524 810522
DESIGNATED STATES: AT; BE; CH; DE; FR; GB; IT; LI; LU; NL; SE
RELATED PARENT NUMBER(S) - PN (AN):
EP 67556 (EP 823025960)
INTERNATIONAL PATENT CLASS: G06F-009/46; G06F-012/14;
ABSTRACT WORD COUNT: 122

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	1018
CLAIMS B	(German)	EPBBF1	868
CLAIMS B	(French)	EPBBF1	1115
SPEC B	(English)	EPBBF1	154256
Total word count - document A			0
Total word count - document B			157257
Total word count - documents A + B			157257

12/3,K/11 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00869025 **Image available**

METHOD FOR PREVENTING DENIAL OF SERVICE ATTACKS
PROCEDE PERMETTANT D'EMPECHER DES ATTAQUES INFORMATIQUES DE TYPE ATTAQUES PAR DENI DE SERVICE

Patent Applicant/Assignee:
NETRAKE CORPORATION, Suite 100, 3000 Technology Drive, Plano, TX 75074, US, US (Residence), US (Nationality)
Inventor(s):
MAHER Robert Daniel III, 7401 Gurney Drive, Plano, TX 75024, US,
BENNETT Victor A, 5565 FM 549, Rockwall, TX 75032, US,
Legal Representative:
NIX Craig J (agent), Netrake Corporation, Suite 100, 3000 Technology Drive, Plano, TX 75074, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200203084 A1 20020110 (WO 0203084)
Application: WO 2001US19492 20010618 (PCT/WO US0119492)
Priority Application: US 2000598631 20000621
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 8028

Fulltext Availability:
Detailed Description
Claims

English Abstract
...do not conform to the predetermined requirements (512) may be dropped (508). The traffic flow scanning engine is further operable to determine whether the data **packets** are associated with **validated traffic flows** (514). Those data **packets** associated with **validated traffic flows** are assigned to a **higher priority** (520) while those not associated with a **validated traffic flow** are assigned to a **low priority** (516), which may occupy no more that a predetermined maximum of the available bandwidth (518).
Detailed Description
... do not verify may be dropped.

After the contents have been verified, the data packets are checked to determine if they are associated with a **validated traffic flow** . If the data **packet** is associated with a **validated traffic flow** it is assigned to a **higher priority** quality of service for transmission back onto the network. If the data **packet** is not associated with a **validated traffic flow** it is assigned to a **low priority** quality of service queue, such that data packets in the **low priority** quality of service queue can occupy no more that a predetermined maximum of the available network bandwidth when they are transmitted back onto the network...

...of service processor uses the conclusion from the traffic flow scanning engine to place the data packets in the appropriate quality of service queue. Data **packets** associated with **validated traffic flow** are placed in **higher priority** queues and transmitted back onto the network according to the protocol for the particular queue. Data **packets** not assigned to a **validated traffic flow** are placed in **low priority** QoS queue. Data packets in the **low priority** QoS queue are transmitted onto the network such that they occupy no more than a predetermined maximum of available bandwidth, thereby preventing flood type DoS...

Claim
... whether the data packets confonn to a set of predetennined

requirements;
fiagging data packets that do not conforin to be dropped;
checking if the data **packets** are associated with a **validated traffic flow** ;
and
assigning data **packets** to a **higher priority** quality of service if the data packet is associat(inverted question mark)d with a **validated traffic flow** and to a **low priority** quality of service if the data **packet** is not associated with a **validated traffic flow** .

8 The network device of Claim. 7 wherein the set of predetermined requirerr.,,ents include packet length, non-overlapping offset fields, and. adherence to protocol...

...a quality of service queue from. a plurality of quality of service queues based on the conclusion from, the traffic flow scanning engine, wherein data **packets** from. non- **validated traffic flows** are assigned to a **low priority** qucue and data **packets** from **validated traffic flow** are assigned to a **higher priority** queue based on its [illegible].

.. The network device of Claim. 12 wherein the **low priority** queue is assigned a
maximum percentage of network bandwidth.

14 The network device of Claim. 12 wherein data packets that do not reorder or reassemble...

12/3,K/12 **(Item 2 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00811796 **Image available**
MPEG RE-MULTIPLEXER HAVING MULTIPLE INPUTS AND MULTIPLE OUTPUTS
REMULTIPLEXEUR MPEG POSSEDANT PLUSIEURS ENTREES ET PLUSIEURS SORTIES
Patent Applicant/Assignee:
GENERAL INSTRUMENT CORPORATION, 101 Tounament Drive, Horsham, PA 19044, US, US (Residence), US (Nationality)
Inventor(s):
ZAUN David Brian, 1016 Salem Road, Cherry Hills, NJ 08034, US,
VIOLA Jeffrey P, 17 Hitchcock Lane, Glen Mills, PA 19342, US,
IAQUINTO Stephen M, 4047 North Mallard Lane, Doylestown, PA 18901, US,
Legal Representative:
[illegible]MEN Ronald (agent), Rader, Fishman & Grauer PLLC, Suite 501, 1233 [illegible] Street, N.W., Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200145419 A1 20010621 (WO 0145419)
Application: WO 2000US34210 20001214 (PCT/WO US0034210)
Priority Application: US 99170531 19991214
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 10154

Fulltext Availability:
Detailed Description

Detailed Description
... this example, timestamps have the highest priority are read first. New packet header information is considered lower priority and CMP packet

data is considered the **lowest priority** . The timestamps are assigned the **highest priority** in the first phase to ensure that the PCR correction calculation will be completed by the time the resultant data is to be inserted into the output packet data stream. As explained above, **packets** having a **valid** PCR filed are detected and flagged by the input processor 120.

Because the input processor 120 will report whether or not a given packet has...

12/3,K/13 **(Item 3 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

WO0211795 **Image available**
HARDWARE FILTERING OF INPUT PACKET IDENTIFIERS FOR AN MPEG RE-MULTIPLEXER
FILTRAGE PAR MATERIEL INFORMATIQUE D'IDENTIFICATEURS DE PAQUETS D'ENTREE, DESTINE A UN REMULTIPLEXEUR MPEG
Patent Applicant/Assignee:
GENERAL INSTRUMENT CORPORATION, 101 Tournament Drive, Horsham, PA 19044, US, US (Residence), US (Nationality)
Inventor(s):
ZAUN David Brian, 1016 Salem Road, Cherry Hills, NJ 08034, US,
VIOLA Jeffrey P, 17 Hitchcock Lane, Glen Mills, PA 19342, US,
TAQUINTO Stephen M, 4047 North Mallard Lane, Doylestown, PA 18901, US,
Legal Representative:
KANANEN Ronald P (agent), Rader, Fishman & Grauer PLLC, Suite 501, 1233 20th Street, N.W., Washington, DC 20036, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200145418 A1 20010621 (WO 0145418)
Application: WO 2000US34209 20001214 (PCT/WO US0034209)
Priority Application: US 99170531 19991214
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
OA BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
AP GH GM KE LS MW MZ SD SL SZ TZ UG ZW
EA AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9896

Fulltext Availability:
Detailed Description

Detailed Description
... example, timestamps have the highest priority are read first. New packet header infon-nation is considered lower priority and CMP packet data is considered the **lowest priority** . The timestamps are assigned the **highest priority** in the first phase to ensure that the PCR correction calculation will be completed by the time the resultant data is to be inserted into the output packet data stream. As explained above, **packets** having a **valid** PCR filed are detected and flagged by the input processor 120.
Because the input processor 120 will report whether or not a given packet has...

12/3,K/14 **(Item 4 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

WO0211794 **Image available**
DYNAMIC CONFIGURATION OF INPUT FILTERING PARAMETERS FOR AN MPEG RE-MULTIPLEXER

CONFIGURATION DYNAMIQUE DE PARAMETRES DE FILTRAGE D'ENTREE POUR UN REMULTIPLEXEUR MPEG

Patent Applicant/Assignee:
GENERAL INSTRUMENT CORPORATION, 101 Tournament Drive, Horsham, PA 19044, US, US (Residence), US (Nationality)

Inventor(s):
[illegible] David Brian, 1016 Salem Road, Cherry Hills, NJ 08034, US,
[illegible]OLA Jeffrey P, 17 Hitchcock Lane, Glen Mills, PA 19342, US,
[illegible]AQUINTO Stephen M, 4047 North Mallard Lane, Doylestown, PA 18901, US,

Legal Representative:
KANANEN Ronald P (agent), Rader, Fishman & Grauer PLLC, Suite 501, 12333 20th Street N.W., Washington, D.C. 20036, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200145417 A1 20010621 (WO 0145417)
Application: WO 2000US33882 20001214 (PCT/WO US0033882)
Priority Application: US 99170531 19991214

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ [illegible] LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG [illegible] SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA
[illegible] AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
[illegible] utility model)) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
[illegible] GH GM KE LS MW MZ SD SL SZ TZ UG ZW
[illegible] AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 9860

Fulltext Availability:
Detailed Description

Detailed Description
... first phase is dictated by the specific data needed to read the packet and the data's relative priority. In this example, timestamps have the **highest priority** are read first. New packet header information is considered lower priority and CMP packet data is considered the **lowest priority** . The timestamps are assigned the **highest priority** in the first phase to ensure that the PCR correction calculation will be completed by the time the resultant data is to be inserted into the output packet data stream. As explained above, **packets** having a **valid** PCR filed are detected and flagged by the input processor 120.

Because the input processor 120 will report whether or not a given packet has...

12/3,K/15 **(Item 5 from file: 349)**
[illegible] File 349:PCT FULLTEXT
[illegible]4 WIPO/Univentio. All rts. reserv.

[illegible]60859 **Image available**
METHOD AND SYSTEM FOR PATH PROTECTION IN A COMMUNICATIONS NETWORK
PROCEDE ET SYSTEME DE PROTECTION DE CHEMINS DANS UN RESEAU DE COMMUNICATION

Patent Applicant/Assignee:
ASTRAL POINT COMMUNICATIONS INC, 19 Alpha Road, Chelmsford, MA 01824, US, US (Residence), US (Nationality)

Inventor(s):
HUMBLET Pierre A, 13 Bigelow Street, Cambridge, MA 02139, US,
MILLER Bruce D, 20 Strawberry Lane, North Reading, MA 01864, US,
SHANMUGARAJ Raj, 253 Hayden Road, Groton, MA 01450, US,
SHERRY Steven, 77 Hillcrest Road, Needham, MA 02492, US,
BEAULIEU Peter B, 3 Suzanne Circle, Plaistow, NH 03865, US,
FORTUNA Michael W, 21 Hawthorne Drive, Fremont, NH 03044, US,
YIP Michael C, 14 Webb Avenue, Wellesley, MA 02481-5431, US,
ABRAHAM William, 15 Galway Road, Windham, NH 03087, US,

Legal Representative:
JOHNSON Rodney D (et al) (agent), Hamilton, Brook, Smith & Reynolds, P.C., Two Militia Drive, Lexington, MA 02421, US,

Patent and Priority Information (Country, Number, Date):
  Patent: WO 200074310 A2-A3 20001207 (WO 0074310)
  Application: WO 2000US15457 20000531 (PCT/WO US0015457)
  Priority Application: US 99324454 19990602; US 2000524479 20000313
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE
  DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC
  LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI
  SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
  (EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
  (OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
  (AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
  (EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 16675

Fulltext Availability:
  Detailed Description

Detailed Description
... lines per niessacre bus. Arbitration is done in a round-robin fashion
  in a centralized arbitration resource located on the system controller
  card 108, with **high - priority** requests given precedence over **low
  priority** requests.
  Each message bus includes the following signals.

  FR **Frame** 604
  15 **VALID** **Valid** bit 612
  SOF Start-of- **frame** 614
  EOF End of frame 616
  DATA[15:01 Data bus signal 61 8
  FC Flow Control 620
  Messages sent over the message bus 102A...

12/3,K/16 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

0532375 **Image available**
DISTRIBUTED FILTERING AND MONITORING SYSTEM FOR A COMPUTER INTERNETWORK
SYSTEME REPARTI DE FILTRAGE ET DE CONTROLE POUR INTERRESEAU INFORMATIQUE
Patent Applicant/Assignee:
  SUN MICROSYSTEMS INC,
Inventor(s):
  GUPTA Amit,
  PERLMAN Radia Joy,
  CHIU Dah-Ming,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9963727 A1 19991209
  Application: WO 99US10272 19990511 (PCT/WO US9910272)
  Priority Application: US 9888348 19980601
Designated States: AL AU BA BB BG BR CA CN CU CZ EE GD GE HR HU ID IL IN IS
  JP KP KR LC LK LR LT LV MG MK MN MX NO NZ PL RO SG SI SK SL TR TT UA UZ
  VN YU GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH
  CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW
  ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 6046
Fulltext Availability:
  Detailed Description

Detailed Description
... the packets. Those packets that have been checked are, according to
  this alternate embodiment, distinguished with an asserted predetermined
  flag 515 and are treated as **high** **priority** packets.

  Specifically, if firewall 200g at an entry point of the trust domain 150

cannot keep up with the incoming traffic, the interior trusted switches 200h need not verify any unverified packets, but rather may choose to treat those packets as **low priority** . That is, those **packets** that are **verified** are placed on **high priority** queues (H 218 of Fig. 2) within a switch 200 and the unverified packets are placed on **low priority** queues (L 214). The **low priority** packets are then prone to "dropping" (discarding) if the trusted region exceeds a certain bandwidth utilization. Thus even though there is not enough CPU capacity...

```
File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200419
         (c) 2004  Thomson Derwent

Set     Items   Description
S1    2217738   TRAFFIC OR PACKET? ? OR FRAME? ? OR DATAGRAM? ? OR FLOW? ?
            OR MESSAGE? ?
S2      47548   (S1 OR DATA OR INFORMATION)(3N)(MALICIOUS OR HARM??? OR DA-
            MAG??? OR DESTRUCTIVE OR UNWANTED OR UNWELCOME OR UNDESIR? OR
            HOSTILE OR DANGER??? OR SUSPECT OR SUSPICIOUS OR ANOMAL? OR M-
            ALEVOLENT OR IRREGULAR? OR ABNORMAL?) OR ATTACK?
S3        516   DENIAL(1W)SERVICE OR TEARDROP OR PING(1W)DEATH OR SMURF
S4       4828   IDS OR NIDS OR INTRUSION? ?(3N)DETECT???
S5      42245   S1(5N)(CHECK??? OR VALIDAT??? OR VERIF???? OR VERIFICATION
            OR ANALYZ? OR ANALYS? OR SCAN???? OR TEST??? OR EXAMIN? OR IN-
            SPECT? OR EVALUAT? OR CERTIF???? OR CERTIFICATION? ?)
S6     238562   HEADER? ? OR OFFSET? ? OR INTEGRITY OR SEQUENCE()NUMBER? ?
            OR CONFORM? ? OR CONFORMITY
S7       3103   QOS OR QUALITY(1W)SERVICE
S8        767   S5(20N)S6
S9         22   S2:S4 AND S8
S10       848   S2:S4 AND S6
S11     15826   S1(10N)S6
S12       161   S2:S4 AND S11
S13      7372   S6(7N)(CHECK??? OR VALIDAT??? OR VERIF???? OR VERIFICATION
            OR ANALYZ? OR ANALYS? OR SCAN???? OR TEST??? OR EXAMIN? OR IN-
            SPECT? OR EVALUAT? OR CERTIF???? OR CERTIFICATION? ?)
S14        81   S2:S4 AND S13
S15        37   S1 AND S14
S16        18   S15 NOT S9
S17       163   S3:S4 AND S6
S18        19   S2 AND S17
S19        15   S18 NOT (S9 OR S16)
S20     40173   S1(5N)(SNIFF??? OR FILTER??? OR SCREEN???)
S21       313   S11 AND S20
S22         5   S21 AND S2:S4
S23       301   S1(5N)VALIDAT?
S24         7   S2:S4 AND S23
S25         6   S24 NOT (S9 OR S16 OR S19 OR S22)
S26        21   S2:S4 AND S7
S27        20   S26 NOT (S9 OR S16 OR S19 OR S22 OR S25)
S28         6   S3 AND S4
S29         4   S28 NOT (S9 OR S16 OR S19 OR S22 OR S25 OR S27)
S30       120   S2 AND S3
S31        94   S30 NOT (S9 OR S16 OR S19 OR S22 OR S25 OR S27 OR S29)
S32        52   S31 AND PACKET? ?
S33      3840   LOW???(2W)PRIORITY
S34      9485   HIGH???(2W)PRIORITY
S35      2211   S33 AND S34
S36        14   S35 AND S2:S4
S37        13   S36 NOT (S9 OR S16 OR S19 OR S22 OR S25 OR S27 OR S29 OR S-
            32)
```

19/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

07605493 **Image available**
INFILTRATION-DETECTING AND INFILTRATION-PREVENTING DEVICE AND PROGRAM THEREFOR

PUB. NO.: 2003-099339 [JP 2003099339 A]
PUBLISHED: April 04, 2003 (20030404)
INVENTOR(s): SHINDO SHUICHI
APPLICANT(s): TOSHIBA CORP
APPL. NO.: 2001-292430 [JP 2001292430]
FILED: September 25, 2001 (20010925)
INTL CLASS: G06F-013/00; G06F-001/00; H04L-012/66

ABSTRACT

PROBLEM TO BE SOLVED: To prevent **attacks** made by **attacking** packets.

SOLUTION: This is an infiltration-detecting and infiltration-preventing device for detecting the infiltration of **attacking** IP packets and preventing the **attack** . In addition, there are provided a firewall function means which refers to a fixed rule representing the relation between the **header** information of preliminarily fixed IP packets, based on the **header** information of the IP packets received and the **attack** , and passes non- **attacking** IP packets, while blocking the **attacking** IP packets; and a filter-type **IDS** function means which passes the non- **attacking** IP packets, while blocking the **attacking** IP packets based on the payload information of the IP packets which pass the firewall function means. The filter-type **IDS** function part 13, different from conventional interception-type **IDS** , can instantly block the **attacking** IP packets.

COPYRIGHT: (C)2003,JPO

19/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

07044154 **Image available**
INTRUSION **DETECTION** DEVICE, SYSTEM, AND ROUTER

PUB. NO.: 2002-252654 [JP 2002252654 A]
PUBLISHED: September 06, 2002 (20020906)
INVENTOR(s): KINOSHITA YOSUKE
APPLICANT(s): MITSUBISHI ELECTRIC CORP
APPL. NO.: 2001-048083 [JP 200148083]
FILED: February 23, 2001 (20010223)
INTL CLASS: H04L-012/66; G06F-013/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide an **intrusion** **detection** device capable of **detecting** an unauthorized access **intrusion** such as DDoS(distributed denial of **service**) **attack** automatically with high accuracy.

SOLUTION: An **intrusion** **detection** unit of a router acquires from a communication route a packet which reaches at the router, and generates a structure corresponding to each session based on network layer data and transport lay data described in the **header** of the packet. This structure is discarded when the session is terminated normally. The **intrusion** **detection** unit inspects the total number n of structures for each prescribed period. If there is any structure with a prescribed threshold nth or more as a result of the inspection, the unit detects it as the unauthorized access intrusion occurrence. Since a structure is generated for each session and the presence/absence of the unauthorized access **intrusion** is **detected** , based on the number of the generated structures, [illegible] **attack** , which establishes a large volume of different sessions, [illegible] detected automatically with high accuracy.

19/5/3 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) Thomson Derwent. All rts. reserv.

Image available
WPI Acc No: 2004-098126/200410
XRPX Acc No: N04-078220

Packet routing control method in Internet applications, involves forwarding packets received at port when source address of packets is conformed to be associated with port

Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE); BRUSTOLONI J A (BRUS-I)
Inventor: BRUSTOLONI J C; BRUSTOLONI J
Number of Countries: 031 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030236999	A1	20031225	US 2002175577	A	20020619	200410	B
EP 1376949	A1	20040102	EP 2002255513	A	20020807	200410	

Priority Applications (No Type Date): US 2002175577 A 20020619
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030236999	A1		10	G06F-011/30	
EP 1376949	A1	E		H04L-012/56	

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Abstract (Basic): US 20030236999 A1

NOVELTY - A packet received at a port is forwarded in a privileged class of service, when the packet source address is affirmatively determined to be properly associated with the port.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) router; and

(2) Internet exchange.

USE - Packet routing control method in Internet for protecting servers from malicious **attacks** such as **denial** of **service** (DoS)

ADVANTAGE - Improving service performance of Internet server by preventing DoS congestive **attacks** . The Internet supporting two classes of services can be prevented.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of system with Internet exchange router.

Internet exchange router (104)

connections (112,113)

pp; 10 DwgNo 1/4

Title Terms: PACKET; ROUTE; CONTROL; METHOD; APPLY; FORWARDING; PACKET; RECEIVE; PORT; SOURCE; ADDRESS; PACKET; **CONFORM** ; ASSOCIATE; PORT
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/30; H04L-012/56
International Patent Class (Additional): H04L-029/06
File Segment: EPI

19/5/4 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

Image available
WPI Acc No: 2003-804194/200375
XRPX Acc No: N03-644654

Node configuring method for facilitating communication, involves generating value in response to request, combining value with information relating to user of node to generate unique address, and allocating address to node

Patent Assignee: BRITISH TELECOM PLC (BRTE)

Inventor: PETRIDIS A; PREVOST S M; VALLI M
Number of Countries: 103 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
WO 200384184 A1 20031009 WO 2003GB1138 A 20030318 200375 B

Priority Applications (No Type Date): GB 200214399 A 20020621; GB 20027231 A 20020327
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
WO 200384184 A1 E 33 H04L-029/12
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): WO 200384184 A1
NOVELTY - The method involves receiving a request for allocation of an address for use by a node for communication, which **conform** to a protocol, and generating a value in response to the request. The generated value is combined with information relating to a user of the node to generate a unique address, and the address is allocated to the node.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) a computer program which, when executed by a processor, performs the method of configuring a node
(b) a tunnel broker for configuring a node.
USE - Used for facilitating communication between hosts through network e.g., Internet.
ADVANTAGE - The method prevents **denial** -of- **service** **attack** by prohibiting the creation of multiple accounts using a single e-mail address. The method sends an account password to the e-mail address provided by the user, thereby prevents registration of a false e-mail address and gaining access to the tunnel broker.
DESCRIPTION OF DRAWING(S) - The drawing shows a schematic diagram of a tunnel broker system.
Tunnels (1)
Node (2)
Tunnel broker (4)
Internet protocol address (11)
Counter address (13)
pp; 33 DwgNo 2/7
Title Terms: NODE; METHOD; FACILITATE; COMMUNICATE; GENERATE; VALUE; RESPOND; REQUEST; COMBINATION; VALUE; INFORMATION; RELATED; USER; NODE; GENERATE; UNIQUE; ADDRESS; ALLOCATE; ADDRESS; NODE
Derwent Class: T01; W01
International Patent Class (Main): H04L-029/12
File Segment: EPI

19/5/5 **(Item 3 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

015600755 **Image available**
WPI Acc No: 2003-662910/200362
XRPX Acc No: N03-529150
Probabilistic packet marking method in network system, involves encoding traceback information using specific bits located in packet header **and terminating traceback path formation when predetermined number of packets are received**
Patent Assignee: ADLER M (ADLE-I); UNIV MASSACHUSETTS (UYMA-N)
Inventor: ADLER M

Number of Countries: 102 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030149777	A1	20030807	US 2002355271	P	20020207	200362	B
			US 2003358123	A	20030204		
WO 200367450	A1	20030814	WO 2003US3240	A	20030204	200363	

Priority Applications (No Type Date): US 2002355271 P 20020207; US
[illegible]358123 A 20030204
[illegible]s:

[illegible] N	Kind	Lan	Pg	Main IPC	Filing Notes
[illegible]	A1		12	G06F-015/173	Provisional application US 2002355271

W[illegible]367450 A1 E G06F-015/16
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT SD SE SI SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): US 20030149777 A1

NOVELTY - The Internet protocol (IP) traceback information is encoded using b bits located in a packet **header** , where b=1. The IP traceback path is formed when packets are received by a destination system. The traceback path is terminated after receiving pre-determined number of packets.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) apparatus for probabilistic packet marking; and

(2) machine-readable medium storing probabilistic packet marking program.

USE - For probabilistic packet marking (PPM) in network system such as packet switching network.

ADVANTAGE - Enables the traceback to occur even when the **header** [illegible] value is one, thereby preventing **denial** of **service** (DoS) **attack** in packet switched network.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram explaining the probabilistic packet marking process.

pp; 12 DwgNo 1/4

Title Terms: PROBABILITY; PACKET; MARK; METHOD; NETWORK; SYSTEM; ENCODE; INFORMATION; SPECIFIC; BIT; LOCATE; PACKET; **HEADER** ; TERMINATE; PATH; FORMATION; PREDETERMINED; NUMBER; PACKET; RECEIVE
Derwent Class: T01; U21; W01
International Patent Class (Main): G06F-015/16; G06F-015/173
International Patent Class (Additional): G06F-015/16
File Segment: EPI

19/5/6 **(Item 4 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015291415 **Image available**
WPI Acc No: 2003-352348/200333
XRPX Acc No: N03-281397
Network attacks **detection method involves parsing data in** intrusion detection **system included in firewall device, to identify data representing text**
Patent Assignee: NETWORKS ASSOC TECHNOLOGY INC (NETW-N)
[illegible]: HERATH N P; MAGDYCH J S; MCDONALD J R; OSBORNE A C; RAHMANOVIC T; [illegible] P E
[illegible] Countries: 001 Number of Patents: 001
[illegible] Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6513122	B1	20030128	US 2001895500	A	20010629	200333	B

Applications (No Type Date): US 2001895500 A 20010629
Details:
Kind Lan Pg Main IPC Filing Notes
B1 12 H04L-009/00

Abstract (Basic): US 6513122 B1
NOVELTY - A portion of data received from a remote source (202), is parsed in an **intrusion detection** system (404) included in a firewall device (210) to identify data representing text. The data representing text is compared to a predetermined list of data representing text, associated with **attacks** to mark the **data** representing text as **hostile** , if match is found.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for gateway system.
USE - For detecting **attacks** such as information gathering **attacks** , web server **denial** of **service** **attack** , file server remote compromise, SYN flood **attack** , IP spoofing, ACK storms, network probes, session hijacking, SNMP **attacks** , ICMP broadcast flooding, land **attack** , ARP **attacks** , ghost routing **attacks** , **sequence number** predict, buffer overflows, mail exploits, authentication race **attacks** , fat ping **attack** , malformed packet **attacks** , forged source address packets, packet fragmentation **attacks** , log overflow **attacks** , log manipulation, source routed packets, DNS cache corruption, mail spamming, DNS **denial** of **service** , FTP bounce or port call **attack** , ICMP protocol tunneling, VPN key generation **attacks** in networks such as LAN, Internet.
ADVANTAGE - The **intrusion** **detection** system efficiently analyzes all incoming data and identifies threats before **hostile** **data** reaches the switched or segmented network.
DESCRIPTION OF DRAWING(S) - The figure shows the firewall architecture.
remote source (202)
firewall device (210)
intrusion **detection** system (404)
pp; 12 DwgNo 4/7
Title Terms: NETWORK; **ATTACK** ; DETECT; METHOD; PARSE; DATA; INTRUDE; DETECT; SYSTEM; FIREWALL; DEVICE; IDENTIFY; DATA; REPRESENT; TEXT
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

19/5/7 **(Item 5 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015264057 **Image available**
WPI Acc No: 2003-324986/200331
XRPX Acc No: N03-260188
Encroachment detection and defense apparatus for network security, allows passage of IP packet not attacked **while interrupting IP packet** attacked , **based on payload information of IP packet which passed**
Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
JP 2003099339 A 20030404 JP 2001292430 A 20010925 200331 B

Applications (No Type Date): JP 2001292430 A 20010925
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
JP 2003099339 A 9 G06F-013/00

Abstract (Basic): JP 2003099339 A
NOVELTY - Based on the **header** information of the received IP packet, the setting rule which shows the relationship between the **header** information of a predetermined IP packet and an **attack** is

referred. A filter-type **IDS** function (13) allows passage of the IP packet which is not **attacked** while interrupting the IP packet which is **attacked** , based on payload information of the IP packet which passed.

USE - Used for network security with respect to unauthorized access and service impossibility **attack** .

ADVANTAGE - Enables defense of internal network from encroachment of unsuitable IP packet.

DESCRIPTION OF DRAWING(S) - The figure shows the structure of the encroachment detection and defense system. (Drawing includes non-English language text)

IDS function (13)

pp; 9 DwgNo 2/10

Title Terms: ENCROACHMENT; DETECT; APPARATUS; NETWORK; SECURE; ALLOW; PASSAGE; IP; PACKET; **ATTACK** ; INTERRUPT; IP; PACKET; **ATTACK** ; BASED; PAYLOAD; INFORMATION; IP; PACKET; PASS

Derwent Class: T01; W01

International Patent Class (Main): G06F-013/00

International Patent Class (Additional): G06F-001/00; H04L-012/66

File Segment: EPI

19/5/8 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015180783 **Image available**

WPI Acc No: 2003-241314/200324

Related WPI Acc No: 2003-241312

XRPX Acc No: N03-192122

Web site protection apparatus from distributed denial-of-services attack **uses server profile enforcement to stop packets not conforming to characteristics of destination and server**

Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE); BRUSTOLONI J A (BRUS-I)

Inventor: BRUSTOLONI J C; BRUSTOLONI J

Number of Countries: 031 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1284573	A1	20030219	EP 2002255511	A	20020807	200324	B
US 20030035370	A1	20030220	US 2001313031	P	20010816	200324	
			US 2002175458	A	20020619		

Priority Applications (No Type Date): US 2002175458 A 20020619; US 2001313031 P 20010816

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1284573	A1	E	18	H04L-029/06	
US 20030035370 A1				H04J-003/14	Provisional application US 2001313031

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Abstract (Basic): EP 1284573 A1

NOVELTY - An Internet service provider (101) has an access gateway (103) incorporating a server profile enforcement unit (102), while plural clients (104) are connected over access links to the gateway and then through the Internet (105) to Internet service providers (106,111). The server profile enforcement unit monitors packets arriving from the clients and drops packets not conforming to the profiles of the destination, such as which protocols are allowed by the server and destination.

DETAILED DESCRIPTION - AN INDEPENDENT CLAIM is included for a web site protection method from **denial** -of- **service** **attack** .

USE - Protecting Internet servers from malicious **denial** -of- **service** **attacks** .

DESCRIPTION OF DRAWING(S) - The drawing shows the system

Service providers (101,106,111)

Server profile enforcement unit (102)

Gateway (103)

Clients (104)
pp; 18 DwgNo 1/5
Title Terms: WEB; SITE; PROTECT; APPARATUS; DISTRIBUTE; SERVICE; **ATTACK** ; SERVE; PROFILE; STOP; PACKET; **CONFORM** ; CHARACTERISTIC; DESTINATION; [illegible]
Derwent Class: T01; W01
International Patent Class (Main): H04J-003/14; H04L-029/06
International Patent Class (Additional): H04L-012/56
File Segment: EPI

19/5/9 **(Item 7 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015030666 **Image available**
WPI Acc No: 2003-091183/200308
XRPX Acc No: N03-072128
Optical signal multicasting method in WDM network, involves transmitting each split version of optical signal over link that is selected based on multicast information in header
Patent Assignee: CHANG G (CHAN-I); CHOWDHURY A M (CHOW-I); ELLINAS G (ELLI-I)
Inventor: CHANG G; CHOWDHURY A M; ELLINAS G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020141409	A1	20021003	US 2001772479	A	20010130	200308	B

Priority Applications (No Type Date): US 2001772479 A 20010130
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020141409	A1		45	H04L-012/28	

Abstract (Basic): US 20020141409 A1
NOVELTY - An optical signal is split optically into two split versions of the optical signal at a node. Each split version of the optical signal is transmitted over a link that is selected based on multicast information in **header** , with reference to local routes.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:
(1) Data payload multicasting method;
(2) **Header** multicasting method;
(3) Optical signal multicasting system;
(4) Optical **header** module; and
(5) Optical **header** processor.
USE - For multicasting optical signal through optical WDM network.
ADVANTAGE - Increases network survivability and bolsters information **integrity** , while mitigating the effects of eavesdropping, misdirection and **denial** of **service attacks** .
DESCRIPTION OF DRAWING(S) - The figure shows a network element for multicasting optical signal.
pp; 45 DwgNo 7/40
Title Terms: OPTICAL; SIGNAL; METHOD; WDM; NETWORK; TRANSMIT; SPLIT; VERSION; OPTICAL; SIGNAL; LINK; SELECT; BASED; INFORMATION; **HEADER**
Derwent Class: W01; W02
International Patent Class (Main): H04L-012/28
File Segment: EPI

19/5/10 **(Item 8 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014584040 **Image available**
WPI Acc No: 2002-404744/200243
Related WPI Acc No: 2002-403590; 2002-415778; 2002-415779; 2002-415791; 2002-415792; 2002-415797; 2002-424967; 2002-425012; 2002-642783

WPI Acc No: N02-317733
Gateway device for computer network, communicates statistics collected from monitor with control center to receive queries or instruction
Patent Assignee: MAZU NETWORKS INC (MAZU-N)
Inventor: KOHLER E W; POLETTO M A
Number of Countries: 097 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200221771	A1	20020314	WO 2001US27413	A	20010904	200243	B
AU 200190612	A	20020322	AU 200190612	A	20010904	200251	

Priority Applications (No Type Date): US 2001931344 A 20010816; US 2000230759 P 20000907
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200221771	A1	E	85	H04L-012/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200190612	A		H04L-012/00	Based on patent WO 200221771	

Abstract (Basic): WO 200221771 A1

NOVELTY - A monitor (33) monitors network traffic through the gateway (26). A communication unit communicates statistics collected in the gateway from the monitor with a control center for receiving queries or instructions. A filter (35) filters out the packets.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Victim site protection method;

(b) Computer program product storing victim site protection program

USE - Gateway device for thwarting **denial** of **service attacks** in computer network.

ADVANTAGE - Information exchange between gateways/data collectors and control center is efficient by transferring the statistical data or minimal **header** information and by compressing all data. By constantly sending more synchronous packets, an **attacker** can effectively prevent server from serving any legitimate connection request. Protects the link between wider internet and the **attacked** data center as well as devices within the data center.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram depicting details of placement of gateway.

Gateway (26)

Monitor (33)

Filter (35)

pp; 85 DwgNo 2/10

Title Terms: GATEWAY; DEVICE; COMPUTER; NETWORK; COMMUNICATE; STATISTICAL; COLLECT; MONITOR; CONTROL; RECEIVE; QUERY; INSTRUCTION
Derwent Class: W01
International Patent Class (Main): H04L-012/00
File Segment: EPI

19/5/11 **(Item 9 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

014408784 **Image available**
WPI Acc No: 2002-229487/200229
XRPX Acc No: N02-176462
Denial -of- service prevention method for Internet Protocol network server involves computing initial sequence number **receiver side by linking random key with TCP connection ID**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: LAMBERTON M; LEVY-ABEGNOLI E; THUBERT P
Number of Countries: 029 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1154610	A2	20011114	EP 2001480023	A	20010315	200229	B
US 20010042200	A1	20011115	US 2001755564	A	20010105	200229	
KR 2001104624	A	20011126	KR 200121222	A	20010419	200231	
TW 518864	A	20030121	TW 2000122332	A	20001024	200356	

Priority Applications (No Type Date): EP 2000480038 A 20000512

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1154610	A2	E	17	H04L-029/06	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
US 20010042200	A1			H04L-009/00	
KR 2001104624	A			H04L-012/22	
TW 518864	A			H04L-029/06	

Abstract (Basic): EP 1154610 A2

NOVELTY - The method listens for reception of SYN message sent from client unit after server TCP activation and when received, computing a **sequence number** receiver side (ISR) and responding with a SYN-ACK message including the ISR. Listening is then resumed. The ISR is computed by linking a randomly generated key with a TCP connection ID that includes client and server sockets.

DETAILED DESCRIPTION - After the ISR computation is executed, the computation is hashed to obtain a server signature, which is linked with a category index referring to a set of predetermined TCP connection categories.

INDEPENDENT CLAIMS are included for:

(1) a system for defeating TCP SYN flooding **attacks** ,

(2) a computer program.

USE - Method is for preventing **denial** -of- **service attacks** (SYN flooding) on Web sites.

ADVANTAGE - Method allows validation of TCP target requests and does not require the allocation of any resources in the target device.

DESCRIPTION OF DRAWING(S) - The figure shows how standard FSM (finite state machine) is changed.

pp; 17 DwgNo 2b/7

Title Terms: SERVICE; PREVENT; METHOD; PROTOCOL; NETWORK; SERVE; COMPUTATION; INITIAL; SEQUENCE; NUMBER; RECEIVE; SIDE; LINK; RANDOM; KEY; CONNECT; ID

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00; H04L-012/22; H04L-029/06

International Patent Class (Additional): H04L-001/00

File Segment: EPI

19/5/12 **(Item 10 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

013627824 **Image available**

WPI Acc No: 2001-112032/200112

XRPX Acc No: N01-161325

Event data packets flow profiling for telephony fraud detection, involves allocating received event data packet to corresponding sub-period, according to time indication in packet

Patent Assignee: NORTEL NETWORKS LTD (NELE)

Inventor: BUTCHART K; DEMPSEY D

Number of Countries: 083 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200146	A1	20001109	WO 2000GB1676	A	20000428	200112	B
AU 2000045884	A	20001117	AU 200045884	A	20000428	200112	
EP 1179260	A1	20020213	EP 2000927481	A	20000428	200219	
			WO 2000GB1676	A	20000428		

Priority Applications (No Type Date): GB 9910268 A 19990504

Patent Details:
Number Kind Lan Pg Main IPC Filing Notes
WO 200067460 A1 E 26 H04M-015/00
Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW
AU 200045884 A H04M-015/00 Based on patent WO 200067460
EP 1179260 A1 E H04M-015/00 Based on patent WO 200067460
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): WO 200067460 A1
NOVELTY - The data defining sub-periods which divide a base time period, is received. A profile of recent behavior of each sub-period, is created. The received event data packet is allocated to corresponding sub-period, according to time indication associated with the packet.
DETAILED DESCRIPTION - The historical profiles of each sub-period, is updated at the end of base time period and recent profile is reset. INDEPENDENT CLAIMS are also included for the following:
(a) method of performing **anomaly** detection in event **data** packet stream;
(b) method of account fraud detection;
(c) method of network **intrusion detection** ;
(d) packet flow profiling system;
(e) anomaly detection system;
(f) account fraud detection system;
(g) network **intrusion detection** system;
(h) program product
USE - For telephony fraud detection using call detail records, **anomaly** detection on **data** streams, network **intrusion detection** using audit log data or IP packet data and for rapid detection of behavioral changes.
ADVANTAGE - The polls of event data can be of any size, allowing the profiles to be produced by the system to maintain their **integrity** . Polls of data for very small periods can be handled easily. The system is suitable for real time and bulk batch feeds of poll data. There is no burden on end user to divide event data into fixed size chunks. The profiles represent the behavior of user, accurately.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of behavioral pattern recognition system.
pp; 26 DwgNo 2/2
Title Terms: EVENT; DATA; PACKET; FLOW; PROFILE; TELEPHONE; FRAUD; DETECT; ALLOCATE; RECEIVE; EVENT; DATA; PACKET; CORRESPOND; SUB; PERIOD; ACCORD; TIME; INDICATE; PACKET
Derwent Class: T01; W01
International Patent Class (Main): H04M-015/00
International Patent Class (Additional): G06F-001/00
File Segment: EPI

19/5/13 (Item 11 from file: 350)
File 350:Derwent WPIX

013386609 **Image available**
WPI Acc No: 2000-558547/200051
XRPX Acc No: N00-413308
Provisioning user's broadband telephony interface in broadband telephony network, involves encrypting and transmitting cryptographic key associated with user to provisioning server
Patent Assignee: AT & T CORP (AMTT)
Inventor: AIELLO W A; BELLOVIN S M; KALMANEK C R; MARSHALL W T; RUBIN A D
Number of Countries: 021 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200052905	A2	20000908	WO 2000US5520	A	20000301	200051	B
EP 1157521	A2	20011128	EP 2000916018	A	20000301	200201	
			WO 2000US5520	A	20000301		

Priority Applications (No Type Date): US 99129476 P 19990415; US 99122481 P 19990301

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200052905	A2	E	23	H04L-029/06	

Designated States (National): BR CA

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

EP 1157521	A2	E	H04L-029/06	Based on patent WO 200052905

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Abstract (Basic): WO 200052905 A2

NOVELTY - The method begins by receiving the information authenticating a provisioning server (140). A communication channel between a user and the provisioning server is then established for transmitting the authorization information from the user to the provisioning server. A cryptographic key, associated with the user, is then encrypted and transmitted to the provisioning server.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for the broadband telephony interface.

USE - Used in a broadband telephony network or with other packet-switched architectures or hybrid network architecture.

ADVANTAGE - Prevents service theft since protections are maintained to limit service to authorized subject to proper accounting. Protects privacy and **integrity** of signaling and media traffic. Protects **integrity** of called number to prevent a range of **attacks** on service including one in which **attacker** tries to steal business from competitor by misrouting calls. Abides by government wire tap laws e.g. Communications Assistance for Law Enforcement Act of 1994. Discourages **denial** of **service attacks** . Provides correct functionality of conventional telephony features. Provides administrative level and levels of privilege to system.

DESCRIPTION OF DRAWING(S) - The figure shows a broadband communication network using the broadband telephony interface provisioning method.

Provisioning server (140)

pp; 23 DwgNo 1/3

Title Terms: USER; BROADBAND; TELEPHONE; INTERFACE; BROADBAND; TELEPHONE; NETWORK; TRANSMIT; CRYPTOGRAPHIC; KEY; ASSOCIATE; USER; SERVE

Derwent Class: W01

International Patent Class (Main): H04L-029/06

File Segment: EPI

19/5/14 **(Item 12 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

012880922 **Image available**

WPI Acc No: 2000-052756/200004

XRPX Acc No: N00-041185

Packets filtering method in networks

Patent Assignee: SUN MICROSYSTEMS INC (SUNM)

Inventor: GUPTA A; PERLMAN R J

Number of Countries: 083 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9955052	A1	19991028	WO 99US6206	A	19990322	200004	B
AU 9931085	A	19991108	AU 9931085	A	19990322	200014	
EP 1074131	A1	20010207	EP 99912788	A	19990322	200109	
			WO 99US6206	A	19990322		
US 6389532	B1	20020514	US 9863630	A	19980420	200239	

JP 2002512487 W 20020423 WO 99US6206 A 19990322 200243
JP 2000545292 A 19990322

Priority Applications (No Type Date): US 9863630 A 19980420

Patent Details:

Patent	Kind	Lan	Pg	Main IPC	Filing Notes
[illegible]	A1	E	35	H04L-029/06	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 9931085	A				Based on patent WO 9955052
EP 1074131	A1	E		H04L-029/06	Based on patent WO 9955052

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

US 6389532	B1			G06F-001/24	
JP 2002512487	W		37	H04L-012/56	Based on patent WO 9955052

Abstract (Basic): WO 9955052 A1

NOVELTY - A packet (300) including a **header** (302) is received by a router. The router determines the existence of a signature (310) in the **header** . The validity of the signature is determined using a public key and the packet is forwarded in accordance with the validity of the signature.

DETAILED DESCRIPTION - The sender of the packet uses a private key obtained from owner to generate the signature. The signature is created by encrypting a fingerprint which corresponds to the data (304) in the packet. The fingerprint is decrypted using the public key of the sender and the decrypted fingerprint is compared with the fingerprint in the [illegible] to check the validity of the signature. The packet is discarded if it has an invalid signature. INDEPENDENT CLAIMS are also included for the following:

(a) packet filtering apparatus;
(b) packet sending apparatus;
(c) packet sending method;
(d) computer program product

USE - For filtering packets in networks.

ADVANTAGE - Avoids wasting router bandwidth and resources on processing packet associated with unauthorized senders. The router filters packets in accordance with a predetermined router limit, such a predetermined rate limit is useful in preventing **denial** of **service attacks** in which an unauthorized sender sends numerous unauthorized packets to the router.

32/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

07789640 **Image available**
DISTRIBUTED **DENIAL** OF **SERVICE** **ATTACK** PREVENTING METHOD, GATE DEVICE, COMMUNICATION DEVICE, AND PROGRAM

PUB. NO.: 2003-283554 [JP 2003283554 A]
PUBLISHED: October 03, 2003 (20031003)
INVENTOR(s): KASHIWA MASARU
ERIC CHEN
FUJI HITOSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)
APPL. NO.: 2002-081904 [JP 200281904]
FILED: March 22, 2002 (20020322)
INTL CLASS: H04L-012/56; H04L-012/46

ABSTRACT

PROBLEM TO BE SOLVED: To limit the transmission band of offensive traffic for a distributed **denial** of **service** (DDoS) **attack** while securing communication traffic for regular users.

SOLUTION: When the **suspicious** offensive **packet** of the DDoS **attack** is detected, a gate device 2001 transmits the suspicious signature and the regular condition of the **suspicious** offensive **packet** to upstream communication devices 2002 and 2003. Each of the communication devices 2002 and 2003 cancels the transmission band limitation of the **packet** identified from the regular condition and a regular signature created based upon the suspicious signature while limiting the transmission band of the **packet** identified from the **suspicious** signature. Further, each of the communication devices 2003 and 2003 transmits the suspicious signature and the regular condition to further upstream communication devices to report the suspicious signature and the regular condition to the upper- most stream communication device in the recursive manner and each communication device further limits the band by detecting the offensive **packet** from the **suspicious** offensive **packets** while implementing the band limitation of the **suspicious** offensive **packet** .

32/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

07296458 **Image available**
METHOD AND SYSTEM FOR PREVENTING DISTRIBUTION TYPE **DENIAL** OF **SERVICE** **ATTACK** AND ITS COMPUTER PROGRAM

PUB. NO.: 2002-164938 [JP 2002164938 A]
PUBLISHED: June 07, 2002 (20020607)
INVENTOR(s): ERIC CHEN
FUJI HITOSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)
APPL. NO.: 2001-274016 [JP 2001274016]
FILED: September 10, 2001 (20010910)
PRIORITY: 2000-276919 [JP 2000276919], JP (Japan), September 12, 2000 (20000912)
2000-276920 [JP 2000276920], JP (Japan), September 12, 2000 (20000912)
INTL CLASS: H04L-012/66; G06F-013/00; H04L-012/56

ABSTRACT

PROBLEM TO BE SOLVED: To provide a device and method for preventing a **denial** of **service** **attack** that can protect itself against the **denial** of **service** **attack** independently of whether or not a sender address is arrogated and to provide a computer program.

SOLUTION: A mobile **packet** filtering program of this invention installed [illegible] router 102 generates a copy of its own program and moves the [illegible] routers 106, 107, 109, 110. The mobile **packet** filtering program [illegible] each router do not pass all traffics sent from hosts 113, 114, [illegible] of distribution type DoS(**Denial** of **Service**) **attackers** to a [illegible] 101. When the **attack** is finished, the mobile **packet** filtering program deletes itself.

32/5/8 (Item 3 from file: 350)

015553099 **Image available**
WPI Acc No: 2004-015929/200402
XRPX Acc No: N04-011981

Network system tracks sending station of attack packet **, when each router detects specific bit pattern and corresponding** attack packet

Patent Assignee: MITSUBISHI ELECTRIC CORP (MITQ)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2003333092	A	20031121	JP 2002138187	A	20020514	200402	B

Priority Applications (No Type Date): JP 2002138187 A 20020514
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003333092	A		9	H04L-012/56	

Abstract (Basic): JP 2003333092 A

NOVELTY - The network system has several routers (11-15, 21-23) that require monitoring of a **packet** with respect to all adjacent routers. The system tracks the sending station of an **attack packet** , when each router detects specific bit pattern and a corresponding **attack packet** .

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) **attack packet** tracking method; and
(2) **attack packet** defense method.

USE - Network system.

ADVANTAGE - The **attack** origin is specified, even when **irregular traffic** by **denial** of **service** (DOS) **attack** is generated. The consumption of network resource by **irregular traffic** , is reduced.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the network system.

edge router (11-15)
core router (21-23)
host (31)
pp; 9 DwgNo 1/2

Title Terms: NETWORK; SYSTEM; TRACK; SEND; STATION; **ATTACK** ; **PACKET** ; ROUTER; DETECT; SPECIFIC; BIT; PATTERN; CORRESPOND; **ATTACK** ; **PACKET**
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/56
International Patent Class (Additional): G06F-013/00
File Segment: EPI

32/5/11 (Item 6 from file: 350)

015786341 **Image available**
WPI Acc No: 2003-848544/200379
XRPX Acc No: N03-678133

Server protection system for Internet, detects source address of client

terminal from which denial **of** service attack **is received, retracts corresponding router and discards** packet **transmitted from client terminal**

Patent Assignee: TOSHIBA KK (TOKE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2003298628	A	20031017	JP 200297051	A	20020329	200379	B

Priority Applications (No Type Date): JP 200297051 A 20020329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003298628	A		5	H04L-012/56	

Abstract (Basic): JP 2003298628 A

NOVELTY - A server (11) processes service requests received from client terminals (13a-13d) through routers (12a-12f). When the server receives **denial** of **service attack** along with service request, the source address of client terminal is detected. The router through which the service request is transmitted is retracted from the detected address, and **packet** transmitted from terminal corresponding to the address is discarded.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) server; and

(2) router.

USE - For protecting server connected to Internet.

ADVANTAGE - Prevents unauthorized access to server by using false address.

DESCRIPTION OF DRAWING(S) - The figure shows the structure of server protection system. (Drawing includes non-English language text).

server protection system (10)
server (11)
routers (12a-12f)
client terminals (13a-13d)
authentication server (14)
pp; 5 DwgNo 1/2

Title Terms: SERVE; PROTECT; SYSTEM; DETECT; SOURCE; ADDRESS; CLIENT; TERMINAL; SERVICE; **ATTACK** ; RECEIVE; RETRACT; CORRESPOND; ROUTER; DISCARDED; **PACKET** ; TRANSMIT; CLIENT; TERMINAL
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/56
File Segment: EPI

32/5/14 **(Item 9 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

Image available
WPI Acc No: 2003-745015/200370
XRPX Acc No: N03-596748

Monitoring device for thwarting denial **of** service attacks **on data center, collects statistical information on** packets **sent between network and data center, by assuming that monitoring device is provided on downstream links**

Patent Assignee: DUDFIELD A E (DUDF-I); POLETTO M A (POLE-I)
Inventor: DUDFIELD A E; POLETTO M A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030145233	A1	20030731	US 200266252	A	20020131	200370	B

Priority Applications (No Type Date): US 200266252 A 20020131
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030145233	A1		18	H04L-009/00	

Abstract (Basic): US 20030145233 A1

NOVELTY - The monitoring device such as a data collector (28) and a gateway (26), collects statistical information on **packets** sent between the network and a data center (20), by assuming that the gateway is provided on downstream links, to examine traffic between a network and the data center.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) method of thwarting **denial** of **service** **attacks** on victim data center; and

(2) arrangement for thwarting **denial** of **service** **attacks** on victim data center.

USE - For thwarting **denial** of **service** **attacks** on computer system in data center.

ADVANTAGE - Provides monitoring capabilities for hosted customers equivalent to placing physical monitors on customer's individual access links.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the computer network.

victim data center (12)
data centers (20a-20c)
control center (24)
gateway (26)
data collector (28)
pp; 18 DwgNo 1/8

Title Terms: MONITOR; DEVICE; SERVICE; **ATTACK** ; DATA; COLLECT; STATISTICAL ; INFORMATION; **PACKET** ; SEND; NETWORK; DATA; ASSUME; MONITOR; DEVICE; DOWNSTREAM; LINK

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00

File Segment: EPI

32/5/15 **(Item 10 from file: 350)**

(ALOGIR)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015682825 **Image available**

WPI Acc No: 2003-745014/200370

XRPX Acc No: N03-596747

Traffic monitoring method for transmission control protocol network, involves building histogram for network parameter to compute outliers in parameter and classify attack

Patent Assignee: GORELIK A (GORE-I); POLETTO M A (POLE-I); RATIN A (RATI-I)

Inventor: GORELIK A; POLETTO M A; RATIN A

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030145232	A1	20030731	US 200266232	A	20020131	200370	B

Priority Applications (No Type Date): US 200266232 A 20020131

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030145232	A1		27	H04L-009/00	

Abstract (Basic): US 20030145232 A1

NOVELTY - The method involves indicating an **attack** on a victim site, if the network parameter values (0 and 1) exceed the normal values. A histogram is built for the parameters to compute outliers in a parameter and classify the **attack** . The network **packets** are filtered based on the characteristics of the **attack** .

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) method for thwarting **denial** of **service** **attacks** on data center;

(2) monitoring device for thwarting **denial** of **service** **attacks** on a data center;

computer program product for network traffic monitoring method;

(4) method of protecting victim site during **denial** of **service attack** ; and

(5) method to reduce blocking of legitimate traffic in process to protect victim site during **denial** of **service attack** .

USE - For monitoring traffic in transmission control protocol (TCP) network, user datagram protocol (UDP), and Internet control message protocol (ICMP) networks.

ADVANTAGE - Determines and detects network **packets** that are portion of **denial** of **service attack** and protects links between the Internet and **attacked** data center.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the network traffic monitoring process.

pp; 27 DwgNo 9/15

Title Terms: TRAFFIC; MONITOR; METHOD; TRANSMISSION; CONTROL; PROTOCOL; NETWORK; BUILD; HISTOGRAM; NETWORK; PARAMETER; COMPUTATION; PARAMETER; CLASSIFY; **ATTACK**

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00

File Segment: EPI

32/5/21 **(Item 16 from file: 350)**

[illegible] File 350:Derwent WPIX

[illegible] Thomson Derwent. All rts. reserv.

[illegible] **Image available**

WPI Acc No: 2003-557056/200352

XRPX Acc No: N03-442690

Packet **transmission control system, has firewall including hardware and software for providing non-redundant connection between networks**

Patent Assignee: COHEN D N (COHE-I); COMPUTING SERVICES SUPPORT SOLUTIONS INC (COMP-N)

Inventor: COHEN D N

Number of Countries: 100 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030084317	A1	20030501	US 20011349	A	20011031	200352	B
WO 200338621	A1	20030508	WO 2002US16312	A	20020520	200352	

Priority Applications (No Type Date): US 20011349 A 20011031

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030084317	A1		11	G06F-011/30	
WO 200338621	A1	E		G06F-011/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

Abstract (Basic): US 20030084317 A1

NOVELTY - The firewalls include hardware and software for providing non-redundant connection (46) between networks (18,22) and for controlling **packet** transmission between networks. The data **packets** (38) received at the firewall are classified based on consumption of resources and the **packet** transmission rate is limited to a maximum acceptable transmission rate (62) associated with each class (66) of received data **packet** .

USE - For managing traffic between networks such as local area networks.

ADVANTAGE - By using the non-redundant network connection, the effects of **packet** flooding and other over usage type distributed **denial** of **service attacks** emanating from inside the local area network, are minimized. Permits the use of insecure public networks in

constructing a wide area network (WAN) that includes both private and public network segments. Maximizes the utilization of data **packet** handling resource within local area network (LAN).

DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the **packet** transmission control system.

traffic (14)
networks (18,22)
computers (26)
communication lines (34)
data **packets** (38)
firewall (42)
non-redundant connection (46)
maximum acceptable transmission rate (62)
class of data **packet** (66)
pp; 11 DwgNo 1/6

Title Terms: **PACKET** ; TRANSMISSION; CONTROL; SYSTEM; FIREWALL; HARDWARE; SOFTWARE; NON; REDUNDANT; CONNECT; NETWORK
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/30
International Patent Class (Additional): G06F-012/14; G06F-015/16; G06F-015/173; H04L-009/00; H04L-009/32
File Segment: EPI

32/5/22 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015494435 **Image available**
WPI Acc No: 2003-556582/200352
XRPX Acc No: N03-442217

General packet **radio service tunneling protocol** packet **filtration method involves dropping data** packets **that do not meet filtering criteria, from signaling messages**

Patent Assignee: KAVANAGH A (KAVA-I); TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: KAVANAGH A
Number of Countries: 101 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030081607	A1	20030501	US 2001336426	P	20011030	200352	B
			US 2002173484	A	20020617		
WO 200339170	A1	20030508	WO 2002IB4493	A	20021029	200352	

Priority Applications (No Type Date): US 2001336426 P 20011030; US 2002173484 A 20020617
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030081607	A1		27	H04L-012/56	Provisional application US 2001336426
WO 200339170	A1	E		H04Q-007/22	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW

Abstract (Basic): US 20030081607 A1

NOVELTY - The general **packet** radio service (GPRS) tunneling protocol (GTP) signaling messages such as GTP path management, GTP tunnel management, GTP mobility management and GTP location management messages are analyzed against many filtering criteria. The data **packets** that do not meet the filtering criteria are dropped while passing the data **packets** that meet the criteria.

USE - For filtering internet protocol (IP) **packets** in general **packet** radio service (GRPS) tunneling protocol (GTP) signaling

messages that are transmitted between GPRS service nodes (GSNs) in GPRS network.

ADVANTAGE - The filtration of IP **packets** limit the effects of **denial** of **service** (DOS) **attacks** , malicious **attacks** session and tunnel hijacking and bandwidth soaked **attacks** on the GTP messages.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart illustrating the GTP **packet** filtration process.

pp; 27 DwgNo 4/17

Title Terms: GENERAL; **PACKET** ; RADIO; SERVICE; PROTOCOL; **PACKET** ; FILTER; METHOD; DROP; DATA; **PACKET** ; FILTER; CRITERIA; MESSAGE

Derwent Class: W01

International Patent Class (Main): H04L-012/56; H04Q-007/22

International Patent Class (Additional): H04L-029/06

File Segment: EPI

32/5/23 **(Item 18 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

015359657 **Image available**

WPI Acc No: 2003-420595/200339

XRPX Acc No: N03-335968

Method for recognizing and refusing denial attacks **involves keeping network connection after receiving acknowledgement signal and forwarding data** packet **after confirming validity of IP connection**

Patent Assignee: GEIS C (GEIS-I); PAUSCH E (PAUS-I); SOYSAL T (SOYS-I)

Inventor: GEIS C; PAUSCH E; SOYSAL T

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030065943	A1	20030403	US 2001966019	A	20010928	200339	B

Priority Applications (No Type Date): US 2001966019 A 20010928

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030065943	A1		20	G06F-011/30	

Abstract (Basic): US 20030065943 A1

NOVELTY - The method involves checking the validity of the registered IP (Internet protocol) connection request and the registered data **packet** . The network connection is kept upon receiving a periodic acknowledgement signal and data **packet** is forwarded to a target system after receiving confirmation of the validity of IP connection request.

DETAILED DESCRIPTION - A computer program run in an electronic intermediary device for implementing a defense against the Dos (**denial** of **service** and DDoS (distributed **denial** of **service**) **attacks** for each IP connection request.

USE - For recognizing and refusing **denial** of **service** or distributed **denial** of **service** **attacks** on server systems.

ADVANTAGE - Provides defense against DoS and DDoS **attacks** on server systems of network system providers, thus computer system is kept stable and efficient over long period.

DESCRIPTION OF DRAWING(S) - The figure is the schematic description of a computer system connected to the Internet.

pp; 20 DwgNo 3/13

Title Terms: METHOD; RECOGNISE; **ATTACK** ; KEEP; NETWORK; CONNECT; AFTER; RECEIVE; ACKNOWLEDGE; SIGNAL; FORWARDING; DATA; **PACKET** ; AFTER; CONFIRM; VALID; IP; CONNECT

Derwent Class: T01

International Patent Class (Main): G06F-011/30

File Segment: EPI

32/5/24 **(Item 19 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

015339118 **Image available**
WPI Acc No: 2003-400056/200338
System for interrupting denial **of** service attack **and method therefor**
Patent Assignee: KT CORP (KTKT-N)
Inventor: KIM S H; PARK S E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2003009887	A	20030205	KR 200144551	A	20010724	200338	B

Priority Applications (No Type Date): KR 200144551 A 20010724
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2003009887	A		1	H04L-012/22	

Abstract (Basic): KR 2003009887 A
NOVELTY - A system for interrupting DoS(**Denial** of **Service**) **attack** and a method therefor are provided to fundamentally interrupt the DoS **attack** by efficiently coping with the DoS **attack** through analysis traffic volume related to a destination address.
DETAILED DESCRIPTION - A host connecting terminal analyzes the current bandwidth by analyzing a protocol of **packets** . The host connecting terminal compares a bandwidth assigned to the corresponding protocol with the current bandwidth. If the current bandwidth of the host connecting terminal is smaller than the assigned bandwidth, the corresponding **packet** is transmitted to a destination. If the current bandwidth of the host connecting terminal is larger than the assigned bandwidth, the corresponding **packet** is abandoned.
pp; 1 DwgNo 1/10
Title Terms: SYSTEM; INTERRUPT; SERVICE; **ATTACK** ; METHOD
Derwent Class: W01
International Patent Class (Main): H04L-012/22
File Segment: EPI

32/5/25 **(Item 20 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015269090 **Image available**
WPI Acc No: 2003-330019/200331
XRPX Acc No: N03-264128
Packets **sequence tracing method in communication network, involves measuring changes in received** packet **rate for each selected network element, in response to application of burst load on network elements**
Patent Assignee: BURCH H J (BURC-I); CHESWICK W R (CHES-I)
Inventor: BURCH H J; CHESWICK W R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030009554	A1	20030109	US 2001901286	A	20010709	200331	B

Priority Applications (No Type Date): US 2001901286 A 20010709
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030009554	A1		11	G06F-015/173	

Abstract (Basic): US 20030009554 A1
NOVELTY - A burst load is applied to each selected network elements such as links, routers. The changes in the received **packet** rate, are measured for the selected network elements, in response to the application of the burst load. A potential source of the **packet** sequence is determined, based on the measured changes.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for **packets** sequence tracing apparatus.
USE - For tracing sequence of **packets** transmitted through

communication networks such as Internet, intranet, LAN, etc.

ADVANTAGE - By the application of burst load to various network elements, the source host of **denial** of **service** (DoS) **attack** to the target host, is determined easily, if the rate is altered upon introduction of the burst load, without co-operation from ISPs along the path.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart explaining the **packets** tracing process.

pp; 11 DwgNo 1/2

Title Terms: **PACKET** ; SEQUENCE; TRACE; METHOD; COMMUNICATE; NETWORK; MEASURE; CHANGE; RECEIVE; **PACKET** ; RATE; SELECT; NETWORK; ELEMENT; RESPOND; APPLY; BURST; LOAD; NETWORK; ELEMENT

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/173

File Segment: EPI

32/5/28 **(Item 23 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015218312 **Image available**

WPI Acc No: 2003-279225/200327

Related WPI Acc No: 2002-405433

XRPX Acc No: N03-221744

Protection against spoofed message DoS attacks for Internet, comprising when receiving DNS request from source IP address for domain name data, intercepting it before delivery and submitting to destination depending on assessed authenticity

Patent Assignee: RIVERHEAD NETWORKS INC (RIVE-N)

Inventor: AFEK Y; GOLAN A; PAZI G; TOUITOU D

Number of Countries: 101 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200325697	A2	20030327	WO 2002IL780	A	20020919	200327	B
US 20030070096	A1	20030410	US 2001929877	A	20010814	200327	
			US 2001323979	P	20010921		
			US 2002251912	A	20020920		

Priority Applications (No Type Date): US 2001323979 P 20010921; US 2001929877 A 20010814; US 2002251912 A 20020920

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200325697	A2	E	38	G06F-000/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW

US 20030070096	A1		G06F-011/30	CIP of application US 2001929877 Provisional application US 2001323979

Abstract (Basic): WO 200325697 A2

NOVELTY - A method for authenticating communication traffic, comprising: receiving a first DNS request comprising data **packets** , sent over a network from a source Internet Protocol (IP) address, to provide network information regarding a given domain name, where receiving the first request comprises intercepting the first request prior to its delivery to a destination IP address, and comprising submitting it to the destination address responsively to the assessed authenticity of the first request, where the information comprises a network IP address associated with the domain name.

DETAILED DESCRIPTION - The method for authenticating communication traffic, also comprising: sending a DNS response to the source address in reply to the first DNS request, the DNS response comprising encoding information in the response, where encoding the information comprises

providing the information in an artificial domain name, and where receiving the second DNS request comprising data **packets** and receiving a query for the network information corresponding to the artificial domain name, and where assessing the authenticity comprises checking the second DNS request for the encoded information; receiving a second DNS request from the source IP address in reply to the DNS response; and assessing authenticity of the first DNS request based on the second DNS request which comprises discarding the first request if it is not assessed to be authentic; if the first request is assessed to be authentic, sending a further DNS response to the source IP address containing the network information corresponding to the domain name. Assessing the authenticity also comprises making a record of the source address as an authentic IP address, and where submitting the first request comprises verifying the source address based on the record, and allowing the network information to be furnished to the verified source IP address.

INDEPENDENT CLAIMS are also included for the following:

(1) An apparatus fro authenticating communication traffic.

(2) A computer program.

USE - Protection against spoofed message, **Denial** -of- **Service** **attacks** in computer networks, where an **attacker** bombards a victim network or server with a large volume of message traffic with the aim of causing a traffic overload that consumes the victims available network bandwidth, CPU capacity, or other critical system resources, and eventually brings the victim's network to a situation in which ii is unable to serve its legitimate clients.

ADVANTAGE - Provides detection of spoofed **packets** (**packets** containing a bogus IP source address, making it difficult for the victim network to defend itself against **attack**) and particularly for distinguishing between spoofed and authentic Domain Name System (DNS) requests.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram that schematically illustrates a network system configured for protection against **Denial** -of- **Service** (DoS) **attacks** .

pp; 38 DwgNo 1/5

Title Terms: PROTECT; MESSAGE; **ATTACK** ; COMPRISE; RECEIVE; REQUEST; SOURCE ; IP; ADDRESS; DOMAIN; NAME; DATA; INTERCEPT; DELIVER; SUBMIT; DESTINATION; DEPEND; ASSESS; AUTHENTICITY

Derwent Class: T01; W01

International Patent Class (Main): G06F-000/00; G06F-011/30

International Patent Class (Additional): G06F-015/173

File Segment: EPI

32/5/29 (Item 24 from file: 350)

DIALOG(R)File 350:Derwent WPIX

015180781 **Image available**

WPI Acc No: 2003-241312/200324

Related WPI Acc No: 2003-241314

XRPX Acc No: N03-192120

Electronic commerce site protection apparatus from distributed denial -of- service attacks **by designating favored clients as very important persons to receive privileged class of service**

Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE); BRUSTOLONI J C (BRUS-I)

Inventor: BRUSTOLONI J C

Number of Countries: 031 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1284558	A1	20030219	EP 2002255516	A	20020807	200324	B
US 20030036970	A1	20030220	US 2001313031	P	20010816	200324	
			US 2002175463	A	20020619		

Priority Applications (No Type Date): US 2002175463 A 20020619; US 2001313031 P 20010816

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes

EP 1284558 A1 E 16 H04L-012/56
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR
US 20030036970 A1 G06F-017/60 Provisional application US 2001313031

Abstract (Basic): EP 1284558 A1

NOVELTY - An Internet service provider (101) supporting two classes of service incorporates VIP gateways (102-104) and plural clients (105) are connected over access links to the gateways. **Packets** are transmitted in both directions and a regular client becomes a selected client when the E-merchant (118) grants a VIP right according to merchant selected criteria and then receives a privileged class of service until revoked by the merchant.

DETAILED DESCRIPTION - AN INDEPENDENT CLAIM is included for a method of protecting electronic commerce sites from **denial** -of- **service attacks** .

USE - Protecting services on the Internet from malicious **attacks** .

ADVANTAGE - Limiting loss from congestion.

DESCRIPTION OF DRAWING(S) - The drawing shows the system

Service provider (101)

Gateways (102-104)

Clients (105)

E-merchant (118)

pp; 16 DwgNo 1/4

Title Terms: ELECTRONIC; SITE; PROTECT; APPARATUS; DISTRIBUTE; SERVICE; **ATTACK** ; DESIGNATED; FAVOUR; CLIENT; IMPORTANT; PERSON; RECEIVE; CLASS; SERVICE
Derwent Class: T01; W01
International Patent Class (Main): G06F-017/60; H04L-012/56
International Patent Class (Additional): H04L-029/06
File Segment: EPI

32/5/30 **(Item 25 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015179399 **Image available**
WPI Acc No: 2003-239929/200323
XRPX Acc No: N03-191093
Authenticating method for packet **communication traffic for computer networks assessing authenticity of source address responsive to value of field indicative of number of hops traversed by** packet **since being sent from source address**
Patent Assignee: RIVERHEAD NETWORKS INC (RIVE-N)
Inventor: BREMLER-BAR A; PAZI G; RIVLIN R; TOUITOU D
Number of Countries: 101 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200319404	A1	20030306	WO 2002IL714	A	20020829	200323 B
US 20030110274	A1	20030612	US 2001316198	P	20010830	200340
			US 2002232993	A	20020829	

Priority Applications (No Type Date): US 2001316198 P 20010830; US 2002232993 A 20020829
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200319404	A1	E	28	G06F-015/173	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW
US 20030110274 A1 G06F-015/16 Provisional application US 2001316198

Abstract (Basic): WO 200319404 A1

NOVELTY - The method involves receiving a data **packet** sent over a network from a source address to a destination address. A value of a field is read from the **packet** that is indicative of a number of hops traversed by the **packet** since having been sent from the source address. Authenticity of the source address is assessed responsive to the value. Assessing the authenticity involves comparing the value of the field to a reference value associated with the source address.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) an apparatus for authenticating **packet** communication traffic;

(b) a computer software product.

USE - For computer networks.

ADVANTAGE - Protects against **denial** of **service** **attacks** in computer networks.

DESCRIPTION OF DRAWING(S) - The figure shows a computer network system.

pp; 28 DwgNo 1/3

Title Terms: AUTHENTICITY; METHOD; **PACKET** ; COMMUNICATE; TRAFFIC; COMPUTER ; NETWORK; ASSESS; AUTHENTICITY; SOURCE; ADDRESS; RESPOND; VALUE; FIELD; INDICATE; NUMBER; HOP; TRAVERSE; **PACKET** ; SEND; SOURCE; ADDRESS

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/16; G06F-015/173

File Segment: EPI

32/5/31 (Item 26 from file: 350)

0050333 **Image available**

WPI Acc No: 2003-091450/200308

XRPX Acc No: N03-072385

Policy management system for networks e.g. internet, determines network policy for each data packet **based on corresponding classification identifier to direct data** packet **according to treatment specified in policy**

Patent Assignee: NETRAKE CORP (NETR-N); CARMAN J R (CARM-I); DEERMAN J R (DEER-I); HERVIN M W (HERV-I); LIE M A (LIEM-I); MAHER R D (MAHE-I); MAXWELL L G (MAXW-I); RANA A V (RANA-I); STROTHER T E (STRO-I)

Inventor: CARMAN J R; DEERMAN J R; HERVIN M W; LIE M A; MAHER R D; MAXWELL L G; RANA A V; STROTHER T E

Number of Countries: 101 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020143948	A1	20021003	US 2001279468	P	20010328	200308	B
			US 2001832670	A	20010411		
WO 200280004	A1	20021010	WO 2002US7506	A	20020314	200308	
EP 1374067	A1	20040102	EP 2002717613	A	20020314	200409	
			WO 2002US7506	A	20020314		

Priority Applications (No Type Date): US 2001279468 P 20010328; US 2001832670 A 20010411

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020143948	A1		16	G06F-015/173	Provisional application US 2001279468
WO 200280004	A1	E		G06F-013/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

EP 1374067 A1 E G06F-013/00 Based on patent WO 200280004

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): US 20020143948 A1

NOVELTY - A processing engine associates each data **packet** received by a network interface with corresponding class identifier. The processing engine retrieves from a database a programmable network policy corresponding to the class identifier and directs the data **packet** through the network according to a treatment specified in the network policy.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for network processing system and management interface.

USE - For performing policy management for networks such as internet providing services such as e-mail, e-commerce, voice over IP (VoIP) and web-browsing.

ADVANTAGE - By determining the proper treatment for each data **packet** , the network identifies and filters out security problems such as e-mail worms, viruses, **denial** of **service** (DoS) **attacks** and illegal hacking. The intelligent network also enables hosting companies and service providers to regulate the bandwidth amount allotted to customers and charge precisely for bandwidth and security features.

DESCRIPTION OF DRAWING(S) - The figure shows the configuration of image builder used in network processing system.

pp; 16 DwgNo 6/7

Title Terms: MANAGEMENT; SYSTEM; NETWORK; DETERMINE; NETWORK; DATA; **PACKET** ; PATH; CORRESPOND; CLASSIFY; IDENTIFY; DIRECT; DATA; **PACKET** ; ACCORD; TREAT; SPECIFIED

Derwent Class: T01

International Patent Class (Main): G06F-013/00; G06F-015/173

International Patent Class (Additional): G06F-015/16; H04Q-011/04

File Segment: EPI

32/5/32 (Item 27 from file: 350)

DIALOG(R)File 350:Derwent WPIX

014807224 **Image available**

WPI Acc No: 2002-627930/200267

XRPX Acc No: N02-496504

Protecting host network against flood-type denial **of** service **attack by comparing received data** packet **with signature to initiate defensive countermeasures**

Patent Assignee: CYBER OPERATIONS LLC (CYBE-N)

Inventor: HSIEH M; LACHMAN J P

Number of Countries: 100 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200271227	A1	20020912	WO 2002US6150	A	20020228	200267 B
US 20020166063	A1	20021107	US 2001272712	A	20010301	200275
			US 200286107	A	20020228	

Priority Applications (No Type Date): US 2001272712 P 20010301; US 200286107 A 20020228

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200271227	A1	E	112	G06F-011/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

US 20020166063 A1 H04L-009/00 Provisional application US 2001272712

Abstract (Basic): WO 200271227 A1

NOVELTY - Method consists in passively collecting a data **packet** from data received by the host network comprising information indicating the **attack** , comparing its information with a signature of an **attack** type and detecting the **attack** . A pathway is provided for

an offensive counter measure against the source of the **attack** .

DETAILED DESCRIPTION - There is an INDEPENDENT CLAIM for a computer program for protecting a host network against a flood-type **denial** of **service attack**

USE - Method is for preventing network flood interruptions without disrupting normal network operations.

DESCRIPTION OF DRAWING(S) - The figure shows a flow chart of the method for detecting and countering a network **attack** .

pp; 112 DwgNo 3/40

Title Terms: PROTECT; HOST; NETWORK; FLOOD; TYPE; SERVICE; **ATTACK** ; COMPARE; RECEIVE; DATA; **PACKET** ; SIGNATURE; INITIATE; DEFENCE

Derwent Class: T01; W01

International Patent Class (Main): G06F-011/30; H04L-009/00

International Patent Class (Additional): G06F-012/14; G06F-015/173; H04L-009/32

File Segment: EPI

32/5/33 **(Item 28 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

014675004 **Image available**

WPI Acc No: 2002-495708/200253

XRPX Acc No: N02-392272

Service refusal attack **prevention method for** packet **communication through internet, involves adding safety identifier to** packet , **depending on degree of safety confirmation and controlling priority based on safety identifier**

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002158699	A	20020531	JP 2000353095	A	20001120	200253	B

Priority Applications (No Type Date): JP 2000353095 A 20001120

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002158699	A		9	H04L-012/56	

Abstract (Basic): JP 2002158699 A

NOVELTY - A safety identifier of specific type is added to the communication **packet** depending on the degree of safety confirmation with respect to the communication **packet** . The priority is controlled based on the safety identifier, by providing a delivery ward on the path of the communication **packet** .

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Service refusal **attack** prevention apparatus;

(2) Service refusal **attack** prevention system; and Recorded medium storing service refusal **attack** prevention program.

USE - For preventing service refusal **attack** or **denial** of **service** (DoS) **attack** for **packet** communication through internet.

ADVANTAGE - Provides countermeasure for an address indeterminate from DOS **attack** .

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of **attack** prevention apparatus. (Drawing includes non-English language text).

pp; 9 DwgNo 1/6

Title Terms: SERVICE; **ATTACK** ; PREVENT; METHOD; **PACKET** ; COMMUNICATE; THROUGH; ADD; SAFETY; IDENTIFY; **PACKET** ; DEPEND; DEGREE; SAFETY; CONFIRM ; CONTROL; PRIORITY; BASED; SAFETY; IDENTIFY

Derwent Class: W01

International Patent Class (Main): H04L-012/56

International Patent Class (Additional): H04L-012/66

File Segment: EPI

32/5/34 (Item 29 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014605228 **Image available**
WPI Acc No: 2002-425932/200245
XRPX Acc No: N02-334925
Denial -of- service attacks **protection system for communication network, determines whether each of** packets **intended for victim device is related to DoS** attack
Patent Assignee: BBNT SOLUTIONS LLC (BBNT-N)
Inventor: DONAGHEY R J
Number of Countries: 096 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200225402	A2	20020328	WO 2001US29336	A	20010919	200245	B
AU 200211242	A	20020402	AU 200211242	A	20010919	200252	

Priority Applications (No Type Date): US 2000666114 A 20000920
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200225402	A2	E	32	G06F-000/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200211242	A		G06F-000/00	Based on patent WO 200225402

Abstract (Basic): WO 200225402 A2
NOVELTY - A service provider (116) receives signal indicating detection of **denial** -of- **service** (DoS) **attack** and **packets** intended for a victim device. A triage device (140) receives the **packets** to determine whether each of the **packets** is related to the DoS **attack** , and forwards the **packets** that are unrelated to the DoS **attack** to the victim device.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) **Denial** -of- **service** **attacks** protection method;
(b) **Denial** -of- **service** **attacks** protecting device;
(c) Computer readable medium storing **denial** -of- **service** **attacks** protection program;
(d) **Attack** detection sensor
USE - For protecting communication networks and devices from **denial** -of- **service** (DoS) **attacks** .
ADVANTAGE - The triage device diverts the brunt of the **attack** from the targets, thereby allowing the targets to continue their operation during DoS **attack** . Even DoS **attacks** that can overwhelm the access link capacity of the target can be handled by the triage device, since the service provider can provide very high capacity access links for this service. The network devices can be configured to automatically detect the DoS **attacks** and trigger the invocation of the triage device and **attacked** hosts can request the invocation of the triage device through any available communication channels.
DESCRIPTION OF DRAWING(S) - The figure shows explanatory view of the explanatory network in which DoS **attack** protection system is implemented.
Service provider (116)
Triage device (140)
pp; 32 DwgNo 1/6
Title Terms: SERVICE; **ATTACK** ; PROTECT; SYSTEM; COMMUNICATE; NETWORK; DETERMINE; **PACKET** ; INTENDED; VICTIM; DEVICE; RELATED; **ATTACK**
Derwent Class: T01
International Patent Class (Main): G06F-000/00
File Segment: EPI

32/5/37 (Item 32 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014595250 **Image available**
WPI Acc No: 2002-415954/200244
Related WPI Acc No: 2002-403556; 2002-403602; 2002-403640; 2002-414499; 2002-415752; 2002-415955; 2002-415956
XRPX Acc No: N02-327279
Denial **of** service attacks **detecting, tracking and blocking system in computer network, includes controller to respond to signals generated by collector and to block specific** data packet flow anomalies
Patent Assignee: UNIV MICHIGAN (UNMI)
Inventor: JAHANIAN F; MALAN G R
Number of Countries: 097 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200221800	A1	20020314	WO 2001US15696	A	20010516	200244	B
AU 200166580	A	20020322	AU 200166580	A	20010516	200251	
EP 1317835	A1	20030611	EP 2001944141	A	20010516	200339	
			WO 2001US15696	A	20010516		

Priority Applications (No Type Date): US 2001855808 A 20010515; US 2000231479 P 20000908; US 2000231480 P 20000908; US 2000231481 P 20000908
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200221800	A1	E	38	H04L-029/06	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200166580	A		H04L-029/06	Based on patent WO 200221800
EP 1317835	A1	E	H04L-029/06	Based on patent WO 200221800

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): WO 200221800 A1
NOVELTY - A collector (20) receives data statistics from the computer network and generates a signal representing **data packet flow anomalies** . A controller (24) responds to the generated signals by tracking attributes related to the **data packet flow anomalies** and blocks specific **data packet flow anomalies** using a filtering mechanism.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for **denial of service attacks** detection, tracking and blocking method.

USE - For detecting, tracking and blocking **denial of service** (DoS) in local and remote computer network such as internet.
ADVANTAGE - Avoids or shuts down the DoS **attack** effectively by blocking **data packet flow anomalies** .
DESCRIPTION OF DRAWING(S) - The figure shows a partially exploded view of a computer network.
Collector (20)
Controller (24)
pp; 38 DwgNo 4/7
Title Terms: SERVICE; **ATTACK** ; DETECT; TRACK; BLOCK; SYSTEM; COMPUTER; NETWORK; CONTROL; RESPOND; SIGNAL; GENERATE; COLLECT; BLOCK; SPECIFIC; DATA; **PACKET** ; FLOW; ANOMALY
Derwent Class: T01; W01
International Patent Class (Main): H04L-029/06
International Patent Class (Additional): H04L-012/26
File Segment: EPI

32/5/38 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014595093 **Image available**
WPI Acc No: 2002-415797/200244
Related WPI Acc No: 2002-403590; 2002-404744; 2002-415778; 2002-415779; 2002-415791; 2002-415792; 2002-424967; 2002-425012; 2002-642783
XRPX Acc No: N02-327122

Data collector for thwart denial of service attack in internet, has sampling device to sample packet traffic, accumulate and collect statistical information about network flow

Patent Assignee: MAZU NETWORKS INC (MAZU-N)
Inventor: KOHLER E W; POLETTO M A
Number of Countries: 097 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200221302	A1	20020314	WO 2001US27402	A	20010904	200244	B
AU 200188687	A	20020322	AU 200188687	A	20010904	200251	

Priority Applications (No Type Date): US 2001931558 A 20010816; US 2000230759 P 20000907
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200221302	A1	E	81	G06F-015/76	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200188687	A		G06F-015/76	Based on patent WO 200221302

Abstract (Basic): WO 200221302 A1

NOVELTY - A computing device samples **packet** traffic, accumulates and collects statistical information about a network flow. The data collectors (28) over a redundant network (30) are linked by a port, to a central control center.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Data collection method;

(b) Computer program product

USE - For thwart **denial** of **service attacks** in internet.

ADVANTAGE - The redundant network is not accessible to the **attacker** . Data collectors are positioned at network switching points, thus the required number of deployed data collectors is minimized.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of placement of the data collectors.

Data collectors (28)

Redundant network (30)

pp; 81 DwgNo 3/10

Title Terms: DATA; COLLECT; SERVICE; **ATTACK** ; SAMPLE; DEVICE; SAMPLE; **PACKET** ; TRAFFIC; ACCUMULATE; COLLECT; STATISTICAL; INFORMATION; NETWORK; FLOW
Derwent Class: T01; W01
International Patent Class (Main): G06F-015/76
International Patent Class (Additional): G06F-011/30
File Segment: EPI

32/5/39 (Item 34 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014595075 **Image available**
WPI Acc No: 2002-415779/200244
Related WPI Acc No: 2002-403590; 2002-404744; 2002-415778; 2002-415791; 2002-415792; 2002-415797; 2002-424967; 2002-425012; 2002-642783
XRPX Acc No: N02-327104

Victim site protecting method in computer network, involves sending

queries to data collectors requesting information to determine source of suspicious network traffic sent to victim
Patent Assignee: MAZU NETWORKS INC (MAZU-N)
Inventor: KOHLER E W; POLETTO M A
Number of Countries: 094 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200221279	A1	20020314	WO 2001US27396	A	20010904	200244	B
AU 200192569	A	20020322	AU 200192569	A	20010904	200251	

Priority Applications (No Type Date): US 2001931487 A 20010816; US 2000230759 P 20000907
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200221279	A1	E	82	G06F-011/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200192569	A		G06F-011/30	Based on patent WO 200221279

Abstract (Basic): WO 200221279 A1

NOVELTY - Queries are sent to data collectors (28) requesting information to determine the source of **suspicious** network **traffic** , indicated by **packets** with faked, random source addresses that change with time, based on victim destination address. A gateway (26) associated with victim data center, in instructed to block **malicious traffic** , when the **attacker** is behind gateway.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for **denial** of **service attack** thwart system.

USE - In computer networks like internet.

ADVANTAGE - By providing a distributed solution to thwarting **denial** of **service attacks** , the **attacks** are stopped near their source, protecting the links between the wider internet and the **attacked** data center as well as devices within the data center. The availability of information from data collectors increases the speed with which the **attackers** are discovered.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of networked computers.

Gateway (26)
Data collectors (28)
pp; 82 DwgNo 1/10

Title Terms: VICTIM; SITE; PROTECT; METHOD; COMPUTER; NETWORK; SEND; QUERY; DATA; COLLECT; REQUEST; INFORMATION; DETERMINE; SOURCE; NETWORK; TRAFFIC; SEND; VICTIM
Derwent Class: T01
International Patent Class (Main): G06F-011/30
International Patent Class (Additional): G06F-012/14; G06F-015/16; G06F-015/173
File Segment: EPI

32/5/40 (Item 35 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014593677 **Image available**
WPI Acc No: 2002-414381/200244
XRPX Acc No: N02-325805
Communication device for distributed denial **of** service attack **management in network, transmits protection module to communication device based on its address extracted with respect to** attack **sources/upstream defense position**
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE); CHEN E Y (CHEN-I); FUJI H (FUJI-I)
Inventor: CHEN E Y; FUJI H

Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020032854	A1	20020314	US 2001948350	A	20010907	200244	B
JP 2002164938	A	20020607	JP 2001274016	A	20010910	200253	

Priority Applications (No Type Date): JP 2000276920 A 20000912; JP 2000276919 A 20000912
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020032854	A1		38	H04L-009/00	
JP 2002164938	A		25	H04L-012/66	

Abstract (Basic): US 20020032854 A1

NOVELTY - A protection module decomposes **packets** , when detected distributed service denial is judged. The addresses of a communication device close to the **attack** sources are identified and are transmitted to the device by transmitter. The address of the device to be chosen at the upstream defense position, is extracted and accordingly a protection module is transmitted.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Communication system;

(b) **Denial** of **service** **attack** protection method;

(c) Recorded medium storing program for defending against distributed **denial** of **service** **attacks**

USE - For managing distributed **denial** of **service** **attacks** in network e.g LAN, internet.

ADVANTAGE - Minimizes the effect of the **attack** **packets** to a locality near the **attack** source and inhibits the harmful effects on the network, thereby communication security is enhanced. Enables countering service **attacks** regardless of legitimacy of the source addresses.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart illustrating procedure for mobile **packet** filtering process.

pp; 38 DwgNo 3/26

Title Terms: COMMUNICATE; DEVICE; DISTRIBUTE; SERVICE; **ATTACK** ; MANAGEMENT ; NETWORK; TRANSMIT; PROTECT; MODULE; COMMUNICATE; DEVICE; BASED; ADDRESS ; EXTRACT; RESPECT; **ATTACK** ; SOURCE; UPSTREAM; POSITION
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00; H04L-012/66
International Patent Class (Additional): G06F-011/30; G06F-013/00; H04L-012/56
File Segment: EPI

32/5/42 (Item 37 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014582936 **Image available**
WPI Acc No: 2002-403640/200243
Related WPI Acc No: 2002-403556; 2002-403602; 2002-414499; 2002-415752; 2002-415954; 2002-415955; 2002-415956
XRPX Acc No: N02-316746

Denial of service attacks detection, tracking and blocking system in computer network, tracks attributes related to data packet flow anomalies to source and block them

Patent Assignee: UNIV MICHIGAN (UNMI)
Inventor: JAHANIAN F; MALAN G R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020032871	A1	20020314	US 2000231479	P	20000908	200243	B
			US 2000231480	P	20000908		
			US 2000231481	P	20000908		
			US 2001855808	A	20010515		

Priority Applications (No Type Date): US 2001855808 A 20010515; US 2000231479 P 20000908; US 2000231480 P 20000908; US 2000231481 P 20000908
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020032871	A1		15	G06F-011/30	Provisional application US 2000231479
					Provisional application US 2000231480
					Provisional application US 2000231481

Abstract (Basic): US 20020032871 A1

NOVELTY - A collector (20) receives and processes the data statistics from the computer network to detect **data packet flow anomalies** and generates signal representing the **data packet flow anomalies** . A controller (24) responds to the signal and tracks the attributes related to the anomalies to the source and blocks the anomalies.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for **denial** of **service** (DoS) **attacks** detection, tracking and blocking method.

USE - For detecting, tracking and blocking **denial** of **service attacks** over local or remote computer networks.

ADVANTAGE - The filtering system allows critical communication services between computer system that deteriorate inter and intra computer system communications. The characteristics related to **denial** of **service attacks** are practical for network engineers and operators to accomplish by inspection alone.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram exemplifying DoS **attack** .

Collector (20)

Controller (24)

pp; 15 DwgNo 7/7

Title Terms: SERVICE; **ATTACK** ; DETECT; TRACK; BLOCK; SYSTEM; COMPUTER; NETWORK; TRACK; ATTRIBUTE; RELATED; DATA; **PACKET** ; FLOW; ANOMALY; SOURCE ; BLOCK
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/30
File Segment: EPI

32/5/43 (Item 38 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014582886 **Image available**
WPI Acc No: 2002-403590/200243
Related WPI Acc No: 2002-404744; 2002-415778; 2002-415779; 2002-415791; 2002-415792; 2002-415797; 2002-424967; 2002-425012; 2002-642783
XRPX Acc No: N02-316696

Denial of service attack protection method in Internet applications, involves sending queries to determine source of suspicious network traffic being sent to victim

Patent Assignee: KOHLER E W (KOHL-I); POLETTO M A (POLE-I)
Inventor: KOHLER E W; POLETTO M A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020032774	A1	20020314	US 2000230759	A	20000907	200243	B
			US 2001931487	A	20010816		

Priority Applications (No Type Date): US 2000230759 P 20000907; US 2001931487 A 20010816
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020032774	A1		49	G06F-015/16	Provisional application US 2000230759

Abstract (Basic): US 20020032774 A1

NOVELTY - The network **packets** with faked source addresses are received and information indicating that victim site is under **attack** ,

is received. The queries are sent to data collectors to request information for determining the source of **suspicious** network **traffic** be sent to victim site.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for system to thwart **denial** of **service** **attacks** on a victim site.

USE - To protect a victim site such as web site or other network site against **denial** of **service** (DoS) **attack** in Internet applications.

ADVANTAGE - Availability of information from data collector increases the speed with which **attackers** are discovered and controls router's behavior when implemented on computer system.

DESCRIPTION OF DRAWING(S) - The figure shows an explanatory view of the technique to gather statistics for use in algorithms that determine sources of **attack** .

pp; 49 DwgNo 7/10

Title Terms: SERVICE; **ATTACK** ; PROTECT; METHOD; APPLY; SEND; QUERY; DETERMINE; SOURCE; NETWORK; TRAFFIC; SEND; VICTIM

Derwent Class: T01; W01

International Patent Class (Main): G06F-015/16

File Segment: EPI

32/5/44 (Item 39 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014562685 **Image available**

WPI Acc No: 2002-383388/200241

XRPX Acc No: N02-300104

Information flow control method in telecommunication system, involves receiving and selectively discarding data packets **based on load constituted by received** packets

Patent Assignee: DEGREE2 INNOVATIONS LTD (DEGR-N); U4EA TECHNOLOGIES LTD (UFOU-N)

Inventor: DAVIES N J; HOLYER J Y; LAFAVE L A; VOWDEN C J

Number of Countries: 095 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200230063	A1	20020411	WO 2000GB3786	A	20001003	200241	B
AU 200075417	A	20020415	AU 200075417	A	20001003	200254	
			WO 2000GB3786	A	20001003		
EP 1327334	A1	20030716	EP 2000964484	A	20001003	200347	
			WO 2000GB3786	A	20001003		
US 20040022193	A1	20040205	US 2003406145	A	20030403	200411	

Priority Applications (No Type Date): WO 2000GB3786 A 20001003

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200230063	A1	E	37	H04L-012/56	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200075417	A		H04L-012/56	Based on patent WO 200230063
EP 1327334	A1	E	H04L-012/56	Based on patent WO 200230063

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

US 20040022193 A1 H04L-001/00

Abstract (Basic): WO 200230063 A1

NOVELTY - The rate of **packet** discard is determined based on the offered load constituted by the received **packets** . The data **packets** are discarded based on an instantaneous approximation of the offered load.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for controller which controls information flow.

USE - Used in telecommunication systems.

ADVANTAGE - If the offered load results in a transported load exceeding the upper threshold level, the transported load may be reduced below the upper threshold level, by selectively discarding **packets** which helps to avoid burst loss and reduces arrival rate of stream. The queue memory and **packet** identifiers ensure that the original position in sequence of each individual **packet** is not lost in the multiplexing operation. There can be different characteristics defined for various load levels that is quality can be up-graded or down-graded as the arrival of rate increases. Thus, the transport characteristics are configured to better match the application requirements to avoid the effects of abnormal offered load e.g. **denial of service attacks** .

DESCRIPTION OF DRAWING(S) - The figure illustrates the principle of defining a transported load in dependence on an offered load in information flow control method.

pp; 37 DwgNo 7/10

Title Terms: INFORMATION; FLOW; CONTROL; METHOD; TELECOMMUNICATION; SYSTEM; RECEIVE; SELECT; DISCARDED; DATA; **PACKET** ; BASED; LOAD; CONSTITUTE; RECEIVE; **PACKET**

Derwent Class: W01

International Patent Class (Main): H04L-001/00; H04L-012/56

International Patent Class (Additional): H04Q-011/04

Document: EPI

32/5/47 **(Item 42 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

014419587 **Image available**

WPI Acc No: 2002-240290/200229

XRPX Acc No: N02-185454

A method of communicating multicast packets **for protecting Internet sites against** denial **of** service attacks **includes selectively varying a chosen multicast address according to a predetermined scheme or by randomly hopping**

Patent Assignee: LADR IT CORP (LADR-N)

Inventor: SHAWCROSS C B A

Number of Countries: 093 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200182548	A2	20011101	WO 2001CA519	A	20010411	200229	B
AU 200152067	A	20011107	AU 200152067	A	20010411	200229	

Priority Applications (No Type Date): US 2000551215 A 20000417

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200182548	A2	E	43	H04L-029/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200152067	A		H04L-029/00	Based on patent WO 200182548

Abstract (Basic): WO 200182548 A2

NOVELTY - A multicast address hopping technique (MAHT) receiver (100) is connected through a router (106) to an autonomous system (104), formed by connected routers of the Internet, and a MAHT transmitter (102) is also connected through a router (108). A chosen multicast Internet Protocol (IP) address is selectively varied according to a predetermined scheme known to the end stations or by randomly hopping between addresses, and communicating **packets** on the chosen IP address.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a system for communicating multicast **packets** between end stations.

USE - The method of communicating multicast **packets** is used for protecting Internet sites against **denial** of **service** **attacks** .

ADVANTAGE - The method prevents unauthorized personnel from knowing which address to disrupt or monitor for traffic between end stations. Addresses are dropped and added to limit the time for an **attacker** . The unicast data received can be filtered and the rate of communicating the multicast **packets** limited to lessen the consumption of the protected site's resources.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic diagram of the general architecture of a system using a multicast hopping technique of communicating multicast **packets** .

MAHT receiver (100)
MAHT transmitter (102)
Autonomous system (104)
Routers (106, 108)
pp; 43 DwgNo 1/9

Title Terms: METHOD; COMMUNICATE; **PACKET** ; PROTECT; SITE; SERVICE; **ATTACK** ; [illegible]; VARY; CHOICE; ADDRESS; ACCORD; PREDETERMINED; SCHEME; RANDOM;

Derwent Class: T01; W01
International Patent Class (Main): H04L-029/00
File Segment: EPI

32/5/48 (Item 43 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014269255 **Image available**
WPI Acc No: 2002-089953/200212
XRPX Acc No: N02-066257

System for anti- denial of service and anti-traffic analysis capabilities for Internet protocol-based virtual private networks and data distribution using Internet protocol multicast address hopping techniques

Patent Assignee: LADR IT CORP (LADR-N)
Inventor: SHAWCROSS C B A
Number of Countries: 093 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200191397	A2	20011129	WO 2001CA727	A	20010522	200212	B
AU 200161957	A	20011203	AU 200161957	A	20010522	200221	

Priority Applications (No Type Date): US 2000575544 A 20000522
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200191397	A2	E	48	H04L-029/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200161957 A H04L-029/00 Based on patent WO 200191397

Abstract (Basic): WO 200191397 A2

NOVELTY - A multicast address hopping technique transmitting site (600) encapsulates original multicast **packets** with a spoofed Internet protocol source address addressed to the range of tunnel exit hosts (608,610,612). Any **packet** arriving at a tunnel host will be de-encapsulated and delivered to receiving sites (614,616,618) with the source of the **packets** selectively varied to conceal the source, while code division multiplexing may be employed to allow various individual destinations to be mixed in one **packet** .

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for methods and systems for transmitting and receiving Internet protocol multicast **packets** .

USE - Providing enhanced virtual private network capabilities on

the Internet.
ADVANTAGE - Protecting against traffic analysis **attacks** .
DESCRIPTION OF DRAWING(S) - The drawing shows a virtual private technique
Transmitting site (600)
Exit hosts (608,610,612)
Receiving sites (614,616,618)
pp; 48 DwgNo 6/9
Title Terms: SYSTEM; ANTI; SERVICE; ANTI; TRAFFIC; ANALYSE; CAPABLE; PROTOCOL; BASED; VIRTUAL; PRIVATE; NETWORK; DATA; DISTRIBUTE; PROTOCOL; ADDRESS; HOP; TECHNIQUE
Derwent Class: W01
International Patent Class (Main): H04L-029/00
File Segment: EPI

32/5/49 **(Item 44 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014081084 **Image available**
WPI Acc No: 2001-565298/200163
XRPX Acc No: N01-420867
Internet Protocol (IP) traceback, for tracing anonymous denial **of** service attacks **, that traces the** attack **back to the node closest to its source**
Patent Assignee: UNIV WASHINGTON (UNIW)
Inventor: ANDERSON T; KARLIN A; SAVAGE S; WETHERALL D
Number of Countries: 094 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200159584	A1	20010816	WO 2001US4373	A	20010209	200163	B
AU 200138134	A	20010820	AU 200138134	A	20010209	200175	

Priority Applications (No Type Date): US 2000181652 P 20000210
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200159584	A1	E	49	G06F-015/163	
AU 200138134	A			G06F-015/163	Based on patent WO 200159584

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

Abstract (Basic): WO 200159584 A1
NOVELTY - Selected data **packets** are marked with the current router's address and any previous address is overwritten. An analysis of a large group of **attacking packets** will enable the node closest to the **attacker** to be determined.
USE - For tracing anonymous **denial** of **service attacks** .
ADVANTAGE - **Attacks** can be eliminated at source during an **attack** .
DESCRIPTION OF DRAWING(S) - The figure shows a flow chart of the traceback process.
pp; 49 DwgNo 2/7
Title Terms: PROTOCOL; IP; TRACE; SERVICE; **ATTACK** ; TRACE; **ATTACK** ; BACK; NODE; CLOSELY; SOURCE
Derwent Class: T01
International Patent Class (Main): G06F-015/163
File Segment: EPI

32/5/52 **(Item 47 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012804490 **Image available**
WPI Acc No: 1999-610720/199952
XRPX Acc No: N99-450021

Denial **of** service **and address spoofing** attacks **blocking method on private network connected to internet**

Patent Assignee: CISCO TECHNOLOGY INC (CISC-N)
Inventor: COX D; MCCLANAHAN K
Number of Countries: 085 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9948303	A2	19990923	WO 99US5900	A	19990318	199952	B
AU 9930982	A	19991011	AU 9930982	A	19990318	200008	

Priority Applications (No Type Date): US 9840898 A 19980318
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9948303	A2	E	15	H04Q-000/00	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 9930982	A		H04Q-000/00	Based on patent WO 9948303

Abstract (Basic): WO 9948303 A2

NOVELTY - The incoming data **packet** from the public network such as internet is analyzed and matched with known patterns associated with known forms of **attack** on the private network. The source of data **packet** is identified as **malicious** or non- malicious based upon the matching.

DETAILED DESCRIPTION - One of the known forms of **attack** is **denial** of **service attack** and the associated known pattern is unacknowledged data **packets** .

USE - For blocking **denial** of **service** and address spoofing **attacks** on private network connected to internet.

ADVANTAGE - Facilitates to identify **denial** of **service attack** and to block such an **attack** from tying up the routing device. Enables routing device to identify address spoofing **attack** and to block such as **attack** using simple technique. Facilitates to track information about **attacker** to allow preventive measures to be taken. If **attack** happens more than once in the same address in the span of certain period of time, then the number of messages can be limited to prevent overloading of E-mail or paging service. Makes use of optional shutdown mechanism to enable routing device to automatically shutdown certain services if **attacks** continued.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the steps involved for blocking **denial** of **service attack** .

```
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 29
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Mar 29
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Mar 29
         (c) 2004 The Gale Group
File  16:Gale Group PROMT(R) 1990-2004/Mar 29
         (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/Mar 29
         (c)2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Mar 29
         (c) 2004 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2004/Mar 27
         (c) 2004 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2004/Mar W2
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Mar W3
         (c) 2004 IDG Communications
File 636:DIALOG Telecom. Newsletters 1995-2004/Mar 25
         (c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/Mar W3
         (c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2004/Mar 29
         (c) 2004 Business Wire.
File 613:PR Newswire 1999-2004/Mar 29
         (c) 2004 PR Newswire Association Inc

Set     Items   Description
S1    3762700   TRAFFIC OR PACKET? ? OR FRAME? ? OR DATAGRAM? ? OR FLOW? ?
            OR STREAM? ?
S2     790502   (S1 OR DATA OR INFORMATION)(3N)(MALICIOUS OR HARM??? OR DA-
            MAG??? OR DESTRUCTIVE OR UNWANTED OR UNWELCOME OR UNDESIR? OR
            HOSTILE OR DANGER??? OR SUSPECT OR SUSPICIOUS OR ANOMAL? OR M-
            ALEVOLENT OR IRREGULAR? OR ABNORMAL?) OR ATTACK?
S3      20909   DENIAL(1W)SERVICE OR TEARDROP OR PING(1W)DEATH OR SMURF
S4      78153   IDS OR NIDS OR INTRUSION? ?(3N)DETECT???
S5     173590   S1(5N)(CHECK??? OR VALIDAT??? OR VERIF???? OR VERIFICATION
            OR ANALYZ? OR ANALYS? OR SCAN???? OR TEST??? OR EXAMIN? OR IN-
            SPECT? OR EVALUAT? OR CERTIF???? OR CERTIFICATION? ?)
S6    1212372   HEADER? ? OR OFFSET? ? OR INTEGRITY OR SEQUENCE()NUMBER? ?
            OR CONFORM? ? OR CONFORMITY
S7       1195   QOS OR QUALITY(1W)SERVICE
S8       3622   S5(15N)S6
S9        116   S3:S4(100N)S8
S10        65   RD (unique items)
S11        29   S10 NOT PY=2001:2004
S12    812314   OFFSET? ? OR SEQUENCE()NUMBER? ? OR CONFORM? ? OR CONFORMI-
            TY
S13     25085   S12(10N)(CHECK??? OR VALIDAT??? OR VERIF???? OR VERIFICATI-
            ON OR ANALYZ? OR ANALYS? OR SCAN???? OR TEST??? OR EXAMIN? OR
            INSPECT? OR EVALUAT? OR CERTIF???? OR CERTIFICATION? ?)
S14        46   S13(100N)S3:S4
S15        28   RD (unique items)
S16        17   S15 NOT (S11 OR PY=2001:2004)
S17       292   VALIDAT?(5N)PACKET? ?
S18         0   S17(20N)S12
S19        30   S2:S4(100N)S17
S20        21   RD (unique items)
S21        10   S20 NOT (S11 OR S16 OR PY=2001:2004)
S22       716   (RULE? ? OR POLICY OR REQUIREMENT? ? OR CRITERIA OR CRITER-
            ION)(5N)PACKET? ?(5N)(CHECK??? OR VALIDAT??? OR VERIF???? OR -
            VERIFICATION OR ANALYZ? OR ANALYS? OR TEST??? OR EXAMIN? OR I-
```

```
              NSPECT? OR EVALUAT? OR CERTIF???? OR CERTIFICATION? ?)
S23       155   S2:S4(100N)S22
S24        66   RD (unique items)
S25        29   S24 NOT (S11 OR S16 OR S21 OR PY=2001:2004)
S26        96   SLEUTH9
S27         0   S26 NOT PY=2001:2004
S28        28   (CONFORM??? OR WELL()BUILT)(7N)PACKET? ?(7N)(CHECK??? OR V-
                ALIDAT??? OR VERIF???? OR VERIFICATION OR ANALYZ? OR ANALYS? -
                OR TEST??? OR EXAMIN? OR INSPECT? OR EVALUAT? OR CERTIF???? OR
                 CERTIFICATION? ?)
S29        17   RD (unique items)
S30        17   S29 NOT PY=2002:2004
S31     17914   LOW???(2W)PRIORITY
S32     98294   HIGH???(2W)PRIORITY
S33      2622   S31(20N)S32
S34        23   S2:S4(100N)S33
S35        18   RD (unique items)
S36       106   PACKET? ?(20N)S7(20N)S31(20N)S32
S37        68   RD (unique items)
S38        42   S37 NOT PD>20000621
```

25/9/29 (Item 4 from file: 610)
DIALOG(R)File 610:Business Wire

00126146 19991025298B0279 (THIS IS THE FULLTEXT)
Phoenix Adaptive Firewall First Linux-Supporting Firewall to Receive I.C.S.A. Certification
Business Wire
Monday, October 25, 1999 09:30 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 774

TEXT:
COLUMBUS, Ohio, Oct 25, 1999 (BUSINESS WIRE) - Progressive Systems, Inc. Achieves Yet Another First
in the Linux Firewall Market

Progressive Systems, Inc., a leading provider of network security solutions, today announced that its Phoenix Adaptive Firewall has received certification from the International Computer Security Association ("ICSA"), the foremost independent evaluation and certification facility for network security products worldwide.

The Phoenix is the first ICSA certified firewall to support Caldera, Red Hat,TurboLinux, and S.u.S.E. Linux distributions, further assuring business customers and value-added resellers (VARs) that Linux is a viable platform for enterprise network security.

"The Phoenix is an enterprise-class security solution for any business concerned with the integrity of its network," said Matt Dawson, President of Progressive Systems. "The Phoenix extends the extreme reliability and high level security of a corporate-grade firewall to all levels of the market. With ICSA certification, businesses and VARs have yet another validation for choosing and recommending the Phoenix."

"ICSA.net is pleased to announce that the Phoenix Adaptive Firewall has passed ICSA Firewall Certification," said Dr. Peter Tippett, Chief Technologist of ICSA.net. "Receiving the certified mark tells business customers that this firewall, when properly configured, can support standard Internet Protocol business services while withstanding an extensive suite of **attacks** . ICSA.net applauds Progressive Systems, Inc. for doing their part to help increase security in the digital world."

The Phoenix Adaptive Firewall gives businesses an enterprise-class, network layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers. In addition, the Phoenix offers secure remote administration through a web GUI. As the only Linux-supporting firewall to be ICSA certified, the Phoenix gives businesses and enterprises the option of making Linux their platform of choice for essential gateway and security services.

Progressive's partners welcomed the groundbreaking certification. "Progressive is the first Linux firewall vendor to recognize the importance of certification," said Benoy Tamang, vice president of Caldera Systems, Inc. "This move strengthens Linux for Business technology, showcasing it as a robust, reliable platform that can run mission critical, gateway apps like Web, VPN and firewall services. The ICSA stamp on the Phoenix firewall is exactly what Linux enterprise customers need to propel deployment because it lays to rest `perceived' Linux security issues -- a big step forward for us all."

"Today's certification is corroboration of what our customers worldwide have already discovered about the Phoenix," continued Dawson. As Doug

Laine of Zdial, Inc., a Philadelphia-ISP, commented, "The Phoenix has performed beyond our expectations. It has truly solved a number of issues for us, and continues to impress us every day. The interface is very easy-to-use and intuitive, and the support has been excellent."

The Phoenix is available for most commercial Linux distributions, including Caldera, Red Hat, S.u.S.E. and TurboLinux, and is also available for the Cobalt RaQ and Rebel.com Netwinder microserver platforms.

ABOUT PROGRESSIVE SYSTEMS, INC.

Progressive Systems, Inc. is a leading vendor of network security and data communications solutions. The company's customer base includes more than 6,000 institutions, governments, and corporations, operating mission-critical applications on all seven continents and in space. The Phoenix Adaptive Firewall is available directly from Progressive Systems or its worldwide network of resellers as either an appliance on the Cobalt RaQ platform or as software for most commercial Linux distributions, including Caldera, Red Hat, S.u.S.E., and TurboLinux. A software add-on is also available for the Cobalt RaQ, RaQ2, Qube, and Qube2 as well as the Rebel.com Netwinder. Headquartered in Columbus, Ohio, Progressive Systems also has offices in San Francisco, CA and Tucson, AZ. Further information is available at http://www.progressive-systems.com or by calling (800) 558-7827.

ABOUT ICSA, INC.

Located in Reston, Virginia, ICSA, Inc. provides Internet security assurance services worldwide. Established in 1989 as an independent corporation, ICSA has successfully led the security industry in the development of high quality security products through product certification programs, and in establishing better security practices through management of multiple security-focused consortia. ICSA certification and security standards are globally accepted. ICSA is an international company and has offices and partners in North America, South America, Europe and Asia. For more information, call (888) 396-8348 or (717) 258-1816 or visit www.icsa.net.

25/9/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02374955 SUPPLIER NUMBER: 59599946 (THIS IS THE FULL TEXT)
WebRamp 700S. (Ramp Networks Inc network security software) (Software Review) (Evaluation)
Internet Magazine, 136
Feb, 2000
DOCUMENT TYPE: Evaluation ISSN: 1355-6428 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 496 LINE COUNT: 00043

TEXT:

Protect your private home or business network using this fully featured firewall

As the prospect affixed high-speed links to the Net draws tantalisingly closer, security becomes even more important. There are several technologies you can use to defend yourself against external **attack** , but a firewall is the most popular.

The WebRamp 700S firewall uses packet filtering to protect your private home or business network, It **examines** incoming and outgoing IP **packet** headers and **checks** its characteristics against a **rules** list that you can create yourself.

Headers contain details about a **packet** 's origin, destination, protocol type, source and destination port number. This lets you build rules about which packets can enter or exit your network.

The WebRamp 700S is a modem-sized product with a handful of status lights at the front and two 10BASE-T ports at the rear. You connect one port to your Internet router and the other to your LAN hub.

Once you're connected to the network, you use a Java-enabled browser to configure the firewall and management functions.

The WebRamp 700S has two extra cost optional extras-support for VPN (from (pounds)279) and CyberNot content filtering (from (pounds)135). When you point your browser at the WebRamp 700S you're greeted with a main status page that summarises your configuration, error messages and the current network status.

The interface has a detailed message log that can be sent to you by email on a regular basis, as well as access to WebRamp's other configuration features. To say this program is highly configurable is an understatement-you can even choose to be emailed when an attack on your network is detected.

The firmware is software upgradeable, so you should keep an eye on the manufacturer's Web site as it posts updates regularly.

The WebRamp 700S operates either in screening mode, where your users have Internet-routable P addresses, or in Network Address Translation (NAT) mode--where they're given private addresses.

By default, the program blocks all incoming connections to computers on your network, but permits all outgoing connections, giving your users transparent network access without direct exposure to the Internet.

The WebRamp uses a 'stateful' inspection model, and protects your network from known 'denial of service attacks. You can open holes in the firewall for individual FTP, SMTP, POP3, ONS and HTTP servers on your network. It's also easy to block various types of activity, including RealAudio, lava applets and cookies.

For businesses in need of firewall protection, the security features of the WebRamp 700s, as well as the easy setup and affordable price, make it easy to recommend.

25/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02446940 SUPPLIER NUMBER: 66686845 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Plan for Growth Without Busting the Budget - Your business may be small now, but you don't want it to stay that way. Here's how to build a network that can grow with you. (Industry Trend or Event)
Schenk, Rob
Computer Shopper, 218
Dec 1, 2000
ISSN: 0886-0556 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2528 LINE COUNT: 00207

... both voice and data traffic, but they're costly.
With any Internet connection comes certain security risks. The best defense against risks such as hacker **attacks** is a firewall. Whether it's hardware- or software-based, a firewall **inspects** every incoming data **packet** , either accepting or denying it based on **rules** the administrator configures. Most firewall products offer some sort of content-filtering capabilities as well, so you can prohibit the viewing of specific types of Web sites by category, such as pornography or violence. More advanced implementations offer **intrusion detection** , virtual-private-networking (VPN) support, and virus-scanning features.
Software firewalls are cheaper than hardware firewalls, but they may be less secure, because they rely...

25/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02437453 SUPPLIER NUMBER: 65637477 (USE FORMAT 7 OR 9 FOR FULL TEXT)
PMC-Sierra to buy SwitchOn. (Company Business and Marketing) (Brief Article)
Electronic Engineering Times, 47
Oct 2, 2000
DOCUMENT TYPE: Brief Article ISSN: 0192-1541 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 197 LINE COUNT: 00020

SwitchOn Networks employs 60 workers in Milpitas, Calif., and 30 in Pune, India. The company said its technology performs complete **inspection** of **packets** up to Layer 7, provides **policy** and content-based networking functions and generates statistics for traffic monitoring and metering.
According to PMC-Sierra, these capabilities are critical for next-generation IP equipment, such as edge routers, aggregation and POP switches, Web switches, network firewalls and **intrusion detection** systems. The transaction will be accounted for as a pooling of interests, PMC-Sierra said.
http://www.eet.com/

25/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02424682 SUPPLIER NUMBER: 63839216 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Preventing the Hack Attack. (Industry Trend or Event)
Rogers, Frank
Communications, 34, 7, 52
July, 2000
ISSN: 0278-4831 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1162 LINE COUNT: 00097

... IP firewall between the internal network of corporate users and any external connection, including an Internet connection. A firewall examines the IP traffic, detects hacker **attack** packets and discards them.

...ques to detect such **attacks** include packet filtering and stateful **inspection** . **Packet** filtering is the simplest approach and uses **rules** to determine which **packets** are discarded. **Rules** are typically based on the source, destination or applications. However, setting up and maintaining filtering rules would be complicated for almost all residential users. In...

25/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02374955 SUPPLIER NUMBER: 59599946 (USE FORMAT 7 OR 9 FOR FULL TEXT)
WebRamp 700S. (Ramp Networks Inc network security software) (Software Review) (Evaluation)
Internet Magazine, 136
Feb, 2000
DOCUMENT TYPE: Evaluation ISSN: 1355-6428 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 496 LINE COUNT: 00043

... speed links to the Net draws tantalisingly closer, security becomes even more important. There are several technologies you can use to defend yourself against external **attack** , but a firewall is the most popular.
The WebRamp 700S firewall uses packet filtering to protect your ... home or business network, It **examines** incoming and outgoing IP **packet** headers and **checks** its characteristics against a **rules** list ... you can create yourself.
Headers contain details about a **packet** 's origin, destination, protocol type, source and destination port number. This lets you build rules about which packets can enter or exit your network.
The...

25/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02204921 SUPPLIER NUMBER: 20974540 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Firewalls for NT survive tough battering. (NetGuard Guardian and Checkpoint Software Technologies Firewall-1) (Software Review) (Evaluation)
Holzbaur, Helen
Government Computer News, v17, n23, p37(1)
July 27, 1998
DOCUMENT TYPE: Evaluation ISSN: 0738-4300 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4624 LINE COUNT: 00394

... a packet filter or an application proxy.
A packet-filtering firewall inspects each packet it receives and ... whether to forward or to drop the **packet** after **checking** a table ... access control **rules** .
... **inspection** , a variation on **packet** filtering, goes beyond ... filtering. It tracks the state of each connection the firewall ... This keeps **attackers** from hijacking a connection while it is ... or closing.
A proxy firewall acts as an intermediary for users. Instead of simply passing along user...
...firewall and then sets up a separate connection to the desired server.
By intercepting all traffic between end points, proxies both reduce the risk of **attack** and allow inspection of data traversing the proxy. Some vendors employ a variation called a circuit relay.
In circuit relay, the user logs in to...

25/3,K/6 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02201990 SUPPLIER NUMBER: 20860682 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Choosing the right firewall architecture environment. (includes related article on Network Security Made Simple) (Enterprise Security) (Technology Information)
Rothke, Ben
Enterprise Systems Journal, v13, n6, p28(6)
June, 1998
ISSN: 1053-6566 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4976 LINE COUNT: 00412

... able to verify whether or not the data was specifically requested. Stateful inspection attempts to track open, valid connection without the need to process a **rule** for each **packet** .

Let's now **examine** the advantages and disadvantages to each architecture.

Packet Filter Advantages:

* Speed
* Sufficient for non-business critical environments
* Generally less expensive
* Flexible
* Transparent
* Can be implemented...

...lacking

* Does not support user authentication
* Can not automatically hide network and system addresses from public view
* Can not provide protection against an application level **attack** (e-mail, Web, Java, etc.)
* Susceptible to sophisticated IP fragmentation and source routing **attacks**
* Can not screen above network layer
* Some protocols do not operate fully in a filters environment (Such as: NFS, NIS/YP, Berkeley "r" commands)
* Can...

25/3,K/7 **(Item 7 from file: 275)**
DIALOG(R)File 275:Gale Group Computer DB(TM)

01989497 SUPPLIER NUMBER: 18693169 (USE FORMAT 7 OR 9 FOR FULL TEXT)
In the line of fire. (firewall technology) (includes related article on breaking language barriers) (Internet/Web/Online Service Information) (Cover Story)
Marve, Anita
LAN Magazine, v11, n11, p62(5)
Oct, 1996
DOCUMENT TYPE: Cover Story ISSN: 1069-5621 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3785 LINE COUNT: 00310

... 2, page 66). The filtering rules include fields such as source and destination IP address, type of protocol, source port number, and destination port number.

Packet filters **examine** these **criteria** against a predefined value and perform a simple comparison before allowing a packet to proceed along its intended route.

Packet filters generally are the least...

...or dropping it. However, packet filters have some major drawbacks: They cannot keep track of a particular network session nor can they prevent IP spoof **attacks** .

IP spoofing occurs when a hacker uses an IP address that belongs to a legitimate, unsuspecting victim--most often someone on the inside of a...

25/3,K/8 (Item 8 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

1905771 SUPPLIER NUMBER: 08536678 (USE FORMAT 7 OR 9 FOR FULL TEXT)
LAN analyzers; building workgroup solutions. (Hardware Review) (overview article to 10 evaluations of local area network analyzers; includes related article on editor's choice) (evaluation)
Derfler, Frank J., Jr.
PC Magazine, v9, n12, p205(19)
June 26, 1990
DOCUMENT TYPE: evaluation ISSN: 0888-8507 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3965 LINE COUNT: 00342

... processing. The top units, like Network General Corp.'s Sniffer, provide an English-language identification of the protocols in use, and evaluate any damage or **irregularities** in the captured **data** .
You can use the protocol analyzer to display packets selectively in real time or to capture activity on the network for later study. Other possibilities include setting filter **criteria** so that the **analyzer** displays only **packets** that are going to or from certain stations, are formatted according to specific protocols, or contain certain errors. Simultaneously setting several of these filters reduces...

25/3,K/9 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

00[illegible] Supplier Number: 65475510 (USE FORMAT 7 FOR FULLTEXT)
PMC-Sierra To Acquire SwitchOn Networks.
Business Wire, p2180
Sept 26, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 644

... speed and make intelligent decisions for applications such as routing, quality of service, load balancing, URL switching, and security. SwitchOn Network's technology performs complete **inspection** of **packets** up to Layer 7, provides **policy** and content based networking and generates statistics for traffic monitoring and metering to allow for value-added services and billing. These capabilities are critical for next generation IP equipment such as edge routers, aggregation and POP switches, web switches, network firewalls and **intrusion detection** systems.
"The addition of SwitchOn Network's packet classification expertise is a complementary fit to our broadband communications strategy," said Bob Bailey, PMC-Sierra's...

25/3,K/10 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

00[illegible] Supplier Number: 61423098 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems Integrates Its Phoenix Adaptive Firewall Onto Cobalt Network's RaQ3i Server Appliance Platform for Easy and Effective Internet Security.
Business Wire, p0141
April 11, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1039

... and Macintosh.
ABOUT PHOENIX
The Phoenix Adaptive Firewall gives businesses an enterprise-class,

network-layer firewall that combines stateful analysis of network traffic with anti- **attack** features to secure business assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributing them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by hackers and offers secure remote administration through a Java GUI. Phoenix also helps protect organizations from distributed **denial** of **service** (DDOS) **attacks** .

The Phoenix firewall appliance, based on the space saving 1U rackmount Cobalt RaQ3i, uses an x86 architecture with a 512k level 2 cache to reach...

25/3,K/11 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02439092 Supplier Number: 60935821 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems and KDD Network Systems Partner to Distribute Linux Firewall Appliance in Japan.
Business Wire, p0193
[illegible], 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1100

... beginning in Q2 of 2000.

About Phoenix

The Phoenix Adaptive Firewall gives businesses an enterprise-class, network-layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributing them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by hackers and offers secure remote administration through a Java GUI.

The Phoenix firewall appliance based on the Cobalt RaQ2 uses a 64...

25/3,K/12 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02432617 Supplier Number: 60267154 (USE FORMAT 7 FOR FULLTEXT)
Moreton Bay and Progressive Systems Partner to Develop Adaptive Firewall Appliance On Embedded Linux Platforms.
Business Wire, p0108
March 20, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 967

... developers can build their solutions.

About Phoenix

The Phoenix Adaptive Firewall gives businesses an enterprise-class, network-layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers and offers secure remote administration through a Java GUI. The Phoenix Adaptive Firewall, the first commercial firewall to support Linux, is...

25/3,K/13 (Item 5 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02302713 Supplier Number: 59124589 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems Delivers Firewall On Cobalt Qube 2.
Business Wire, p1152
Feb 2, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1068

... from the ground up with security in mind. The Phoenix is an enterprise-class, network layer firewall that combines state and packet analysis with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers. As the only Linux-supporting firewall to be both ICSA and LinuxLabs certified, the Phoenix gives businesses and enterprises the option...

25/3,K/14 (Item 6 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02301521 Supplier Number: 59113333 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems' Phoenix Adaptive Firewall Appliance Certified ``Linux-Ready'' by Linuxcare Labs.
Business Wire, p1574
Feb 1, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 861

... security services.
About the Phoenix Firewall Appliance
The Phoenix Adaptive Firewall gives businesses an enterprise-class, network layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers and offers secure remote administration through a Java GUI.
The Phoenix firewall appliance based on the Cobalt RaQ2 uses a 64...

25/3,K/15 (Item 7 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02113802 Supplier Number: 55087273 (USE FORMAT 7 FOR FULLTEXT)
Network-1 Security Solutions Joins With Microsoft to Enhance Security of Windows NT.
Business Wire, p1243
July 7, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 790

... based application and infrastructure services to be more network secure than comparative UNIX offerings. CyberwallPLUS-SV provides industrial-strength, multi-level security that includes stateful **packet inspection** and detailed network access controls for address-mapping, time-based **rules** , and filtering capabilities. The product detects and actively protects Windows NT-based servers against malicious **denial** -of-**service** and intrusion **attacks** , and other "suspicious" network activity.
Tactical Remote Access Penetration Study (TRAPS) TRAPS is a fixed price external network penetration service which provides crucial

information on...

25/3,K/16 (Item 8 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01870574 Supplier Number: 54598379 (USE FORMAT 7 FOR FULLTEXT)
Hi/fn & NetBoost Form Alliance to Deliver Wire-Speed, Policy-Based VPN Platforms.
Business Wire, p0235
May 11, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 467

... wire-speed IP Security (IPSec) encryption/compression processors. They will meet the processing demands of network applications such as firewalls, routers, access concentrators, VPN gateways, **intrusion detection** systems and resource load balancers.
"This important alliance will result in robust security throughout the corporate network for functions that need to be performed at wire [illegible] such as **policy** -based **packet inspection** , encryption and [illegible]," said Ray Farnham, chairman and CEO of Hi/fn. "The work we are [illegible] with NetBoost is a win for OEMs and...

25/3,K/17 (Item 9 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01760315 Supplier Number: 53236579 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems, Inc. Announces Availability of the Phoenix Adaptive Firewall for Linux; Includes Java-based Secure Remote Administration Tool.
Business Wire, p1418
Nov 18, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 454

... gateway applications such as web, VPN and firewall services."
The Phoenix Adaptive Firewall provides a granular level of Security, protecting networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrator. Inbound data with non-allowed contents is not transmitted to the network being protected. This provides a very fine-grained...

... firewalls implemented today. Users can achieve greater precision in [illegible] access to networks than is possible with traditional firewalls. [illegible] Firewall Technology includes anti- **attack** features, disabling [illegible] probing **attacks** commonly used by crackers.
The Phoenix Adaptive Firewall also features an easy-to-use Secure Remote Administration via a Java GUI. This interface provides strong...

25/3,K/18 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07880174 Supplier Number: 65810491 (USE FORMAT 7 FOR FULLTEXT)
PMC-Sierra switches on.
Electronics Times, p10
Oct 2, 2000
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 122

Privately-held SwitchOn's technology performs complete **inspection** of Internet Protocol (IP) **packets** up to Layer 7. It provides **policy** - and content-based networking and monitors traffic for metering purposes.

These capabilities are critical for edge routers, aggregation and point- of-presence switches, Web switches, network firewalls and **intrusion detection** systems.

Bob Bailey, PMC-Sierra's chairman and chief executive, said: "The addition of SwitchOn's packet classification expertise is a complementary fit to our...

25/3,K/19 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

[illegible] Supplier Number: 64434784 (USE FORMAT 7 FOR FULLTEXT)
LinuxWorld to offer plenty of menu items.(Product Announcement)
[illegible], Phil
Network World, p16
August 14, 2000
Language: English Record Type: Fulltext
Article Type: Product Announcement
Document Type: Magazine/Journal; General Trade
Word Count: 620

... oil industries. Smiley says he'd like to see more integrated and easily manageable Linux security and administration tools.

"If a new type of (hacker) **attack** comes, you have to gather the **packets** , **analyze** them and create your own new **rules** every time," Smiley says. "It'd be nice if there was a way to automate that."

Caldera will debut Cosmos, its first network management product...

25/3,K/20 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06198629 Supplier Number: 54128805 (USE FORMAT 7 FOR FULLTEXT)
Linux gets its first firewall.(Progressive Systems' Phoenix Adaptive Firewall software for Linux)(Product Announcement)
Government Computer News, v18, n6, p64(1)
March 15, 1999
Language: English Record Type: Fulltext
Article Type: Product Announcement
Document Type: Magazine/Journal; Tabloid; Trade
Word Count: 125

The Phoenix firewall **inspects** incoming **packets** and distributes them according to **rules** established by the administrator. Inbound data can be blocked, and there are anti- **attack** features to stop common types of **attacks** . The Java graphical interface allows remote administration and is designed to provide strong authentication and encryption from the Web browser.

The charge for an unlimited...

25/3,K/21 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06007776 Supplier Number: 53404239 (USE FORMAT 7 FOR FULLTEXT)
Combine approaches for ultimate security.(overview of test of network security solutions)(Hardware Review)(Software Review)(Evaluation)
InfoWorld, v20, n50, pNA(1)
Dec 14, 1998
Language: English Record Type: Fulltext
Article Type: Evaluation

Publication Type: Magazine/Journal; Trade
Word Count: 753

... the firewall. This technology, called stateful inspection, examines protocol information to verify that a given connection is part of a legitimate conversation.

Stateful inspection thwarts **attacks** that hobble packet filters and may equal or surpass the security of proxied access because it also examines information through application-layer commands.

Also, because...

...do not process the logic of client/server interactions, they typically operate faster than their proxy counterparts. Does superior performance sacrifice flawless security? Theoretically, yes: **Packet inspection** engines pass **packets** unmodified if access **rules** permit, but proxies intercept, **validate** , and rewrite all information before sending it on. But the marketplace has answered this question with a resounding "no." No gaping flaws yet have been...

25/3,K/22 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10406795 SUPPLIER NUMBER: 21033831 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Windows NT-based firewalls. (data security features)
Stewart, Helen
Computer Dealer News, v14, n28, p37(2)
July 24, 1998
ISSN: 1184-2369 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2050 LINE COUNT: 00165

... Windows NT, we have one thing to say to those experts: Guess again.

NSTL bombarded seven top-selling NT firewalls with nearly 300 forms of **attack** and found no significant security loopholes. These products also do an excellent job of locking down potential vulnerabilities in Windows NT itself. Two products stood...

...an application proxy. A packet-filtering firewall inspects each packet it receives and makes the decision to forward or drop the traffic based on a **check** against a table of access control **rules** . Stateful **inspection** , a variation on **packet** filtering, goes beyond simple filtering by also keeping track of the state of each connection the firewall handles.

A proxy firewall acts as an intermediary for users. By intercepting all traffic between endpoints, proxies not only reduce the chance for **attack** but also allow inspection of data traversing the proxy.

After years of debate over which technology offers better security, vendors are beginning to blend the...

25/3,K/23 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10790767 SUPPLIER NUMBER: 20790767 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Red-hot firewalls. (computer network security)
Gittleson, Howie; Sharp, Ron; Cheswick, Bill
America's Network, v102, n10, p48(4)
May 15, 1998
ISSN: 1075-5292 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3065 LINE COUNT: 00246

... a smart packet filter can apply more complex rules and monitor not just individual packets but entire sessions, creating more rigorous and flexible defenses against **attacks** .

The smart filter reads the header of a session's first packet, compares it to the rules and, if approved, routes successive packets through a...

...filter compares its header to that of the first packet to verify that it belongs to the same session. Thus, it doesn't need to **verify** each **packet** against the **rules** .

With information about entire sessions, a smart- **packet** -filter firewall can deploy very secure means to control unauthorized access. One strategy is to control otherwise wide-open UDP connections by forcing UDP sessions...

25/3,K/24 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01223772 CMP ACCESSION NUMBER: EET20001002S0038
PMC-Sierra to buy SwitchOn
ELECTRONIC ENGINEERING TIMES, 2000, n 1134, PG47
PUBLICATION DATE: 001002
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: BUSINESS
WORD COUNT: 176

SwitchOn Networks employs 60 workers in Milpitas, Calif., and 30 in Pune, India. The company said its technology performs complete **inspection** of **packets** up to Layer 7, provides **policy** and content-based networking functions and generates statistics for traffic monitoring and metering.

According to PMC-Sierra, these capabilities are critical for next-generation IP equipment, such as edge routers, aggregation and POP switches, Web switches, network firewalls and **intrusion detection** systems. The transaction will be accounted for as a pooling of interests, PMC-Sierra said.

http://www.eet.com/

25/3,K/25 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01151510 CMP ACCESSION NUMBER: NWC19980115S0022
SOHO Firewall Routers: ISDN Branch Office Security
Mark Fratto
NETWORK COMPUTING, 1998, n 901, PG102
PUBLICATION DATE: 980115
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Reviews
WORD COUNT: 4245

... Systems' AS5300, using Multilink PPP, was employed to terminate the ISDN calls and route calls to our enterprise network.

To test security, we generated spoofing **attacks** using Internet Security Systems' Firewall Scanner package. All of the devices performed as advertised, allowing only the traffic we defined to pass through the firewall...

...Chariot end points were smaller than 127 bytes to maximize the amount of work each SOHO firewall router had to process. We then added filtering **rules** to the devices and ran the same **tests** .

Even with **packet** -filtering **rules** enabled, the performance hit was less than 2 percent. Finally, compression was turned on and the same tests were repeated.

25/3,K/26 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00371024 20000926270B7379 (USE FORMAT 7 FOR FULLTEXT)
PMC-Sierra To Acquire SwitchOn NetworksAcquisition Adds High-Spee Classification and Packet Processing Expertise for Internet Protocol (IP) Routing and Addresses New Market Segments Including Web Switches and Security Systems
Business Wire
Tuesday, September 26, 2000 08:01 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 640

...speed and make intelligent decisions for applications such as routing, quality of service, load balancing, URL switching, and security. SwitchOn Network's technology performs complete **inspection** of **packets** up to Layer 7,
provides **policy** and content based networking and generates statistics for traffic monitoring and metering to allow for value-added services and billing.
These capabilities are critical for next generation IP equipment such as edge
routers, aggregation and POP switches, web switches, network firewalls and **intrusion detection** systems.

"The addition of SwitchOn Network's packet classification expertise is a complementary fit to our broadband communications strategy," said Bob Bailey,
PMC-Sierra's...

25/3,K/27 (Item 2 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00246546 20000403094B6701 (USE FORMAT 7 FOR FULLTEXT)
TheLinuxStore.com Now Offers the Full Line of Progressive Systems Linux-based Firewall and VPN Solutions
Business Wire
Monday, April 3, 2000 08:05 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,169

...CE), Solaris and Macintosh.

ABOUT PHOENIX

The Phoenix Adaptive Firewall gives businesses an enterprise-class, network-layer firewall that combines packet state analysis with anti-**attack**
features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and filtering them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable
networking probe **attacks** commonly used by hackers and offers secure remote
administration through a Java GUI. Phoenix also helps protect organizations from distributed **denial** of **service** (DDOS) **attacks** .

The Phoenix firewall appliance based on the award-winning Cobalt RaQ2 uses a
64 bit, 250mhz RISC processor to reach performance levels above T-3...

25/3,K/28 (Item 3 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00155640 19991213347B1429 (USE FORMAT 7 FOR FULLTEXT)
Progressive Systems Announces Free Giveaway of Linux Firewall; Phoenix Adaptive Firewall Personal Use Version Available for Download Today
Business Wire
Monday, December 13, 1999 11:03 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 709

...ABOUT THE PHOENIX FIREWALL

The Phoenix Adaptive Firewall gives businesses of all sizes an enterprise-class, network layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers. In addition, the Phoenix offers secure remote administration through a Java Graphical User Interface (GUI). As the only Linux-supporting firewall...

25/3,K/29 (Item 4 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00126146 19991025298B0279 (USE FORMAT 7 FOR FULLTEXT)
Phoenix Adaptive Firewall First Linux-Supporting Firewall to Receive I.C.S.A. Certification
Business Wire
Monday, October 25, 1999 09:30 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 774

...the certified mark tells business customers that this firewall, when properly configured, can support standard Internet Protocol business services while withstanding an extensive suite of **attacks** . ICSA.net applauds Progressive Systems, Inc. for doing their part to help increase security in the digital world."

The Phoenix Adaptive Firewall gives businesses an enterprise-class, network layer firewall that combines state tracking with anti- **attack** features to secure network assets. The Phoenix protects networks by performing a detailed **inspection** of all aspects of incoming **packets** and distributes them according to **rules** determined by the network administrators. The firewall also includes anti- **attack** features that disable networking probe **attacks** commonly used by crackers. In addition, the Phoenix offers secure remote administration through a Java GUI. As the only Linux-supporting firewall to be ICSA...

38/9/8 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07614557 Supplier Number: 62241557 (THIS IS THE FULLTEXT)
Global Watch.(Technology Information)
Greenfield, David
Network Magazine, pNA
Feb 1, 2000
ISSN: 1093-8001
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 745

ABSTRACT:
Frame relay continues to evolve despite the fact that IP is more flexible and ATM is faster. It has been enhanced in performance, combined with QoS and most recently blended with IP to link multiple sites and run high-end applications with the necessary bandwidth. AT&T's new IP Enabled Frame Relay has revitalized interest in the technology by letting companies deploy meshed frame networks at far less cost than alternative technologies. Companies pay for permanent virtual circuits (PVC) between pairs of sites, typically in a hubbed configuration to reduce the number of circuits. IP Enabled Frame users order a special PVC running from a Cisco router and take advantage of the carrier's adoption of Multiprotocol Layer Switching (MPLS) on the IP backbone. AT&T's network contains a Cisco PBX frame switch that converts frame packets into IP and marks them with MPLS tags before sending them to their destination.
TEXT:
The gods must have a special place for frame relay. Bested by ATM in speed and by IP in flexibility, frame relay keeps on mutating and growing. First there was high-speed frame. Then there was frame with QoS. Now the frame-meisters are blending IP with frame to make it better than ever at linking scads of sites and running top-class apps.

The latest remake has two episodes. Episode one: the AT&T story. The carrier rolled out IP Enabled Frame Relay in the United States in January [illegible]. The technology enables companies to deploy meshed frame networks at [illegible]tom prices.

Here's how it works. Today, companies wiring up a WAN with frame relay pay for Permanent Virtual Circuits (PVCs) between pairs of sites. Growing the number of sites and interconnecting offices to each other requires a huge number of PVCs. A 10-site network, for example, would demand 45 PVCs for a fully meshed network. To avoid that cost, companies end up wiring in a hubbed configuration, connecting sites to a central headquarters. While this architecture might create a single point of failure and introduce additional latency, it reduces those 45 PVCs, for example, to just nine.

With IP Enabled Frame, AT&T has a way to cut full-meshed network costs. The key is the adoption of the Multiprotocol Layer Switching (MPLS) protocol on AT&T's IP backbone. MPLS delivers frame-like PVCs on top of IP with one exception: those circuits can encompass multiple sites.

Customers looking to mesh their networks order a special PVC from AT&T that runs from a Cisco Systems router on the customer premises to the Cisco BPX frame switch on AT&T's network. The BPX converts the frame packets into IP, marks the packets with an MPLS tag, and sends them across AT&T's IP backbone to their destination.

The only catch is reliability. Network managers must base their frame network on a single vendor, and as experience shows, no frame relay network is foolproof. This is particularly true as AT&T looks to deliver the service internationally through Concert, its partnership with British Telecom. "If you've suffered the number of breakdowns in the network that I have, then you wouldn't want to connect major sites with just one vendor," says Toni Bergman, network manager at SKF AB, a bearings manufacturer.

Episode two: the Nortel Networks story. The frame switch provider has come out with two enhancements for managed IP-over-frame services. Dubbed IP Enhanced Frame Relay, Nortel technology aims to solve the configuration and QoS issues of running IP over frame relay.

On the configuration side, the company has devised a way to shorten

upgrade times on managed IP-over-frame services. Normally upgrading a frame PVC requires reconfiguring the switch and the routers on both ends of the PVC. With the Nortel approach, changes made to the PVC at the frame switch are automatically pushed down to the Customer Premises Equipment (CPE), which reconfigures itself. The feature works with routers from Nortel subsidiary Bay Networks, but that may change soon. Nortel says it has proposed the configuration technology to the frame relay forum, which may decide to adopt the spec in the first quarter of 2000.

On the **QoS** side, Nortel has implemented differentiated QoS over a single PVC. Current frame relay QoS, from providers like Infonet Service (www. infonet.com), assigns applications with different priorities to different circuits. Mission-critical applications, for example, might be assigned to better performing (and more expensive) PVCs, while less important applications would be assigned to **lower - priority** PVCs. However, none of these services can give **higher priority** to a CEO browsing the Web than they can to the janitor.

Nortel's new **QoS** initiative will enable carriers to make that distinction. The product now uses **QoS** levels assigned by the router on the customer premises. **QoS** levels are designated through the differentiated services specification. Once tagged by the router, the **packets** get placed in a queue associated with that service level. **High - priority packets** are placed in a queue serviced more frequently than **packets** in a **low - priority** queue.

Just when these features will find their way into services isn't clear. "We want to statically configure our CPE gear to ensure parameters are set correctly," says Brian Presley, frame relay product manager at Infonet. And the **QoS** features? "We aren't currently looking for **QoS** over a single PVC," says Presley. "The ability to set up different PVCs gives us more flexibility and better control over the network."

38/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

[illegible] SUPPLIER NUMBER: 58374348 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Nortel Networks Leads the Pack With Accelar Enterprise Switch. (the Accelar 8600) (Hardware Review) (Evaluation)
[illegible]over, Joel
Network Computing, 16
Dec 27, 1999
DOCUMENT TYPE: Evaluation ISSN: 1046-4468 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1186 LINE COUNT: 00097

... load. Because of Accelar's shared memory architecture, the switch latency remains constant regardless of load or port configuration.

Finally, I tested the switch's **QoS** (**Quality** of **Service**) capabilities. Using two ports to oversubscribe a third, I tested its priority queuing mechanism. I offered varying loads of **low** - and **high** - **priority** traffic, and in all cases the Accelar forwarded 100 percent of the **high** - **priority** traffic without any **packet** loss.

I applaud Nortel's decision to include support for eight hardware-based priority queues in the 8600 architecture. The vendor's support for eight classes of service allows for a significant amount of **QoS** granularity in the enterprise backbone.

The icing on the cake for the Accelar 8600 is its aggressive pricing. Nortel has taken huge strides toward making...

38/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

[illegible]34 SUPPLIER NUMBER: 55730211 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lucent delivers DSL with Stinger. (Lucent Technologies DSL access concentrator) (Company Business and Marketing)
Hersch, Warren S.
Computer Reseller News, 26
Sept 13, 1999
ISSN: 0893-8377 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 521 LINE COUNT: 00046

... the technology. The offering also is currently in trials at more than 20 customers worldwide.

The product received a mixed reaction from resellers.

"(Stinger's) **QoS** and **packet** prioritization features are what it takes to do voice-over-DSL deployments," said Jeff Carnegie, president of Carnegie Technical Inc., a San Diego-based VAR, adding the product's release was an inevitable step. "But I don't believe any of the routers on the market support **QoS** . And, regarding DSL quality, the router's ability to differentiate between **high** - **priority** and **low** - **priority** **packets** is key," he said.

"This is not a channel product," said Randy Wear, principal of Decisions Systems Plus Inc., a Rosemont, Ill.-based VAR. "An...

38/3,K/3 (Item 3 from file: 275)
[illegible](R)File 275:Gale Group Computer DB(TM)
[illegible] The Gale Group. All rts. reserv.

[illegible] SUPPLIER NUMBER: 20786419 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Fly my way: ATM's efficiency challenge. (Technology Information)
Huang, Alan; Moreland, Chuck
Telephony, v234, n23, p22(1)
June 8, 1998
ISSN: 0040-2656 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1776 LINE COUNT: 00152

... starvation when higher-class traffic exceeds the available bandwidth. This problem has the potential to escalate into serious congestion as the source retransmits delayed IP **packets** .

Advanced traffic management avoids bandwidth starvation by allowing a service provider to assign each service class a minimum bandwidth guarantee. This reduces the **QOS** effect on **lower - priority** traffic of the temporary presence of excess **higher - priority** traffic, just as some discount fare seats are available on all flights.

A common pool of bandwidth can be set aside and shared on a...

38/3,K/4 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

02238790 Supplier Number: 57648945 (USE FORMAT 7 FOR FULLTEXT)
N.E.T. Offers Higher Performance in Frame Relay Switching for Multiservice Networks.
PR Newswire, p9936
Nov 19, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 673

... ideal for multiservice networks. Network operators can optimize network efficiency and tailor network traffic to support multiple levels of service and meet their end-users **QoS** requirements. For example, a **higher priority** level of access can be assigned to delay-sensitive applications, such as voice and video, while a **lower priority** level of access is assigned to data and image applications that are more tolerant of network delays. Through a sophisticated algorithm, FPQ minimizes the **packet** loss, ensures the reliability of **high priority** traffic and prevents **lower priority** traffic from being "locked out" -- even during congestion.

The new fragmentation feature of the FRX is suitable for service provider networks that support a mixture...
...voice and video, and requiring different levels of delivery. On a per PVC basis, fragmentation enables service providers to control the maximum size for the **packets** that are queued into the network. This improves **QoS** through lower delay variation of **high priority** , delay sensitive traffic (small frame) when mixed with **low priority** , non-delay sensitive (large frame) traffic. Segmented **packets** traverse the network, segment-by-segment, and are reassembled before leaving the FRX network.

N.E.T.'s seamless LMI offers greater session resiliency and...

38/3,K/5 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

01421918 Supplier Number: 46680721 (USE FORMAT 7 FOR FULLTEXT)
Ipsilon Adds Fast Ethernet Backbone Capability to IP Switched Networks; Expands IP Switching Software Feature Set; New FAS1200 Product Raises the Bar for Fast Ethernet Price/performance.
Business Wire, p09030047
Sept 3, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1269

... or destination address, service type, or transport protocol. Because it takes advantage of information already contained in the header, Ipsilon's flow classification process delivers **QoS** as an integral benefit of IP switching technology, enabling managers to switch data streams to particular ATM ports for priority forwarding.

Using flow classification, each IP Switch can steer **packets** onto an ATM virtual connection with a **QoS** appropriate to the application. For example, if the flow is a time-critical stock market data feed, it could receive the **highest priority** through the ATM fabric; conversely, the

flow might contain an experimental video service that should be treated with the **lowest priority** .

The key benefit to the local policy **QoS** supported by the new Ipsilon software is that applications need not be rewritten to comply with ATM Forum standards; instead, the TCP/IP information in the IP **packet** can set up the appropriate **QoS** .

Managers can configure local policy within the IP Switched network using the graphical user interface provided by Ipsilon's Network Voyager, a Web-based network...

38/3,K/6 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

04494174 Supplier Number: 57771521 (USE FORMAT 7 FOR FULLTEXT)
N.E.T.: N.E.T. offers higher performance in frame re relay switching for multiservice networks.
M2 Presswire, pNA
[illegible], 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 716

... ideal for multiservice networks. Network operators can optimize network efficiency and tailor network traffic to support multiple levels of CoS and meet their end-users **QoS** requirements. For example, a **higher priority** level of access can be assigned to delay-sensitive applications, such as voice and video, while a **lower priority** level of access is assigned to data and image applications that are more tolerant of network delays. Through a sophisticated algorithm, FPQ minimizes the **packet** loss, ensures the reliability of **high priority** traffic and prevents **lower priority** traffic from being "locked out"-- even during congestion.

The new fragmentation feature of the FRX is suitable for service provider networks that support a mixture...
...voice and video, and requiring different levels of delivery. On a per PVC basis, fragmentation enables service providers to control the maximum size for the **packets** that are queued into the network. This improves **QoS** through lower delay variation of **high priority** , delay sensitive traffic (small frame) when mixed with **low priority** , non-delay sensitive (large frame) traffic. Segmented **packets** traverse the network, segment-by-segment, and are reassembled before leaving the FRX network.

N.E.T.'s seamless LMI offers greater session resiliency and...

38/3,K/7 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03256219 Supplier Number: 46681047 (USE FORMAT 7 FOR FULLTEXT)
-IPSILON NETWORKS: Ipsilon adds fast ethernet backbone capability to IP switched networks
M2 Presswire, pN/A
Sept 3, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1304

... or destination address, service type, or transport protocol. Because it takes advantage of information already contained in the header, Ipsilon's flow classification process delivers **QoS** as an integral benefit of IP switching technology, enabling managers to switch data streams to particular ATM ports for priority forwarding.

Using flow classification, each IP Switch can steer **packets** onto an ATM virtual connection with a **QoS** appropriate to the application. For example, if the flow is a time-critical stock market data feed, it could receive the **highest priority** through the ATM fabric; conversely, the flow might contain an experimental video service that should be treated

... **lowest priority** .

The key benefit to the local policy **QoS** supported by the new Ipsilon software is that applications need not be rewritten to comply with ATM or LAN standards; instead, the TCP/IP information in the IP **packet** can set up the appropriate **QoS** .

Managers can configure local policy within the IP Switched network using the graphical user interface provided by Ipsilon's Network Voyager, a Web-based network...

38/3,K/8 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

00614557 Supplier Number: 62241557 (USE FORMAT 7 FOR FULLTEXT)
Global Watch. (Technology Information)
Greenfield, David
Network Magazine, pNA
Feb 1, 2000
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 745

... has proposed the configuration technology to the frame relay forum, which may decide to adopt the spec in the first quarter of 2000.

On the **QoS** side, Nortel has implemented differentiated QoS over a single PVC. Current frame relay QoS, from providers like Infonet Service (www. infonet.com), assigns applications with...

...different circuits. Mission-critical applications, for example, might be assigned to better performing (and more expensive) PVCs, while less important applications would be assigned to **lower - priority** PVCs. However, none of these services can give **higher priority** to a CEO browsing the Web than they can to the janitor.

Nortel's new **QoS** initiative will enable carriers to make that distinction. The product now uses **QoS** levels assigned by the router on the customer premises. **QoS** levels are designated through the differentiated services specification. Once tagged by the router, the **packets** get placed in a queue associated with that service level. **High - priority packets** are placed in a queue serviced more frequently than **packets** in a **low - priority** queue.

Just when these features will find their way into services isn't clear. "We want to statically configure our CPE gear to ensure parameters are set correctly," says Brian Presley, frame relay product manager at Infonet. And the **QoS** features? "We aren't currently looking for **QoS** over a single PVC," says Presley. "The ability to set up different PVCs gives us more flexibility and better control over the network."

38/3,K/9 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

00614459 Supplier Number: 62241440 (USE FORMAT 7 FOR FULLTEXT)
Global Watch. (IP with frame) (Company Business and Marketing)
Greenfield, David
Network Magazine, pNA
Jan 1, 2000
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 745

... has proposed the configuration technology to the frame relay forum, which may decide to adopt the spec in the first quarter of 2000.

On the **QoS** side, Nortel has implemented differentiated QoS over a single PVC. Current frame relay QoS, from providers like Infonet Service (www. infonet.com), assigns applications with...

...different circuits. Mission-critical applications, for example, might be assigned to better performing (and more expensive) PVCs, while less important applications would be assigned to **lower - priority** PVCs. However, none of these services can give **higher priority** to a CEO browsing the Web than they can to the janitor.

Nortel's new **QoS** initiative will enable carriers to make that distinction. The product now uses **QoS** levels assigned by the router on the customer premises. **QoS** levels are designated through the differentiated services specification. Once tagged by the router, the **packets** get placed in a queue associated with that service level. **High - priority packets** are placed in a queue serviced more frequently than **packets** in a **low - priority** queue.

Just when these features will find their way into services isn't clear. "We want to statically configure our CPE gear to ensure parameters are set correctly," says Brian Presley, frame relay product manager at Infonet. And the **QoS** features? "We aren't currently looking for **QoS** over a single PVC," says Presley. "The ability to set up different PVCs gives us more flexibility and better control over the network."

38/3,K/10 **(Item 3 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07299715 Supplier Number: 61866424 (USE FORMAT 7 FOR FULLTEXT)
Chipset supports Gigabit Layer 3/4 Ethernet switches. (Brief Article)
Electronics Times, p55
April 25, 2000
Language: English Record Type: Fulltext
Article Type: Brief Article
Document Type: Magazine/Journal; Trade
Word Count: 234

... linking multiple chips or design a variety of switches by linking to other devices in the Allayer series.

The switch supports key features such as **quality** of **service**, trunking and Vlan. The device supports four classes of service which allows a networking switch to recognise and give priority to **packets** of data that have been marked for faster delivery. The device recognises and prioritises class 0 (management information), class 1 (voice and video), class 2 (data) and class 3 (back-up data), which are examples of **high** to **low priority** rating.

The trunking feature in the AL1022 supports IEEE 802.3ad. This feature enables multiple ports on a switch to be combined into faster connection...

38/3,K/11 **(Item 4 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07060459 Supplier Number: 59474641 (USE FORMAT 7 FOR FULLTEXT)
Full speed ahead. (Hardware Review) (Evaluation)
Bell, Steve
Network World, v15, n42, p76
Oct 19, 1998
Language: English Record Type: Fulltext
Article Type: Evaluation
Document Type: Tabloid; Trade
Word Count: 2613

... We're not convinced this approach will enhance routing protocol performance, but time will tell.

The SSR-16 is capable of routing 30 million IP **packet**/sec via its nonblocking switch fabric. The switch provides dedicated, independent **packet** buffers on each output port, and space is allocated for hundreds of maximum-size Ethernet **packets** on each Fast Ethernet and Gigabit port. Separate buffer space is allocated to each of four classes of traffic, and

forwarding is done on a prioritized basis, ranking the four classes from **highest** to **lowest** **priority** .

Cabletron takes an excellent approach to **QoS** , and we believe four [illegible] an appropriate number of levels. Many vendors offer too few or too many classes; two is too few, and...

38/3,K/12 **(Item 5 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)

06756732 Supplier Number: 56894968 (USE FORMAT 7 FOR FULLTEXT)
Caught Up On Video? -- Video is about to become a big part of corporate networking. Here's how net architects can prepare for the show. (Internet/Web/Online Service Information)
Fritz, Jeffrey
Data Communications, p51
Oct 21, 1999
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 2756

... services as Diffserv (differentiated services), IP precedence, MPLS (multiprotocol label switching), RSVP (resource reservation protocol), and 802.1p are helping improve things on the IP **QOS** front (seeTable 2).

QOS , Continued

To process different priority levels, a switch or router must be constructed with multiple queues for every port. Queues are like holding tanks for the various priority levels, and when there's more than one, higher - **priority** **packets** can be prioritized and moved ahead of traffic [illegible] **lower** **priority** level.

Unfortunately, many switches and routers have single queues only. When there's congestion, all **packets** begin lining up in the same queue-which isn't good as far as video is concerned. So try to upgrade switches and routers so...

38/3,K/13 **(Item 6 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)

06441642 Supplier Number: 55009157 (USE FORMAT 7 FOR FULLTEXT)
Two Switches Top Layer 3 Field. (Extreme's Black Diamond 6800 beats Foundry's BigIron 8000) (Hardware Review) (Evaluation)
Conover, Joel
Network Computing, p73
June 28, 1999
Language: English Record Type: Fulltext
Article Type: Evaluation
Document Type: Magazine/Journal; Trade
Word Count: 2254

... in order for each priority. Out-of-order packets are counted, but reported separately. Upon completion of the test run, QoSBench compares the number of **packets** received at each priority level with the expected number of **packets** received at that priority level, and assigns a QoS [illegible] based on the number of **packets** received in order.

The IEEE 802.1p standard specifies that QoS be delivered strictly on a strict-priority basis. In QoSBench, this means that if four priority levels are offered to the DUT, all the **highest** - **priority** information should arrive, to the exclusion of **lower** - **priority** traffic. The QoS factor provided by QoSBench takes this into account. If the DUT drops any **high** - **priority** frames, the DUT receives no credit for meeting the QoS agreement for the **lower** - **priority** queues.

If the device under test passes all the **packets** it possibly can, in order, and with proper QoS, it is possible for the device to exceed a 100-percent QoS factor. **Packets** buffered by the DUT at lower priorities will be expelled from the queues of the device after all **higher** - **priority**

packets have been forwarded. These buffered packets also count toward the QoS factor if all other QoS guarantees have been met. Both of the devices we...

...of QoS guarantees.

First, the Priority Test measured the switch's ability to forward IEEE 802.1Q tagged VLAN frames properly while enforcing Layer 4 **QoS** based on the IEEE 802.1p bits defined inside the tagged frame. This test validates the switch's ability to handle 802.1Q tagged frames...

...to each port with a unique UDP source and destination port number. The switch was configured to filter traffic that would have gone into the **highest - priority** queue, and the remaining traffic was to be classified into the three **lower - priority** levels. This test stressed the DUT's ability to filter traffic while maintaining **QoS** . It also forced vendors to use the lower three queues in their architecture to the exclusion of the **highest - priority** queue. Thus, if the vendor were "cheating" by allocating additional memory to the **highest - priority** queue, it would become apparent in this test. Both products properly enforced **QoS** while filtering all **packets** configured to be discarded. The results are summarized in "Filtering Test Results" below.

It should be noted that both vendors had to do some tweaking...

38/3,K/14 **(Item 7 from file: 16)**
DIALOG(R)File 16:Gale Group PROMT(R)

06328543 Supplier Number: 54596363 (USE FORMAT 7 FOR FULLTEXT)
Empowering Policy -- What's the verdict in the industry's first test of Layer 4 switches? Qualified success in adding QOS to TCP apps. But until latency and jitter are brought under control, these boxes can't be considered the cornerstone of the corporate network.(Hardware Review)(Evaluation)
Mandeville, Robert; Newman, David
Data Communications, p60(1)
May 7, 1999
Language: English Record Type: Fulltext Abstract
Article Type: Evaluation
Document Type: Magazine/Journal; Trade
Word Count: 4442

... to control TCP. Several vendors told us our capabilities were more advanced than their internal testing mechanisms and gave them a deeper understanding of how **QOS** works.

Time and Punishment

We conducted four sets of tests. First, we offered steady-state traffic and took baseline measurements of forwarding rate with no...
...post office protocol version 3) data over TCP port 110; the balance were low-priority HTTP sessions using TCP port 80. Both high- and low- **priority** sessions transferred 1 Mbyte of TCP data over the backbone.

Because traffic from 10 fast Ethernet ports is theoretically capable of being carried by a...Ethernet backbone.

To find out if QOS can help, we headed back to the test bed. This time we asked vendors to enable QOS so **high - priority** traffic would receive four times the bandwidth of **low priority** . Then we offered the switches the same load as in the prior round: nine **high - priority** and 18 **low - priority** TCP sessions to each of 16 inbound ports.

We were mainly interested in determining if forwarding rates for **high - priority** traffic improve with QOS enabled. We also were curious to see what would happen to **low - priority** traffic-would switches deliver a 4:1 ratio?

Activating QOS made a difference for all switches-but there were big variations. Lucent's Cajun pushed **high** -priority **packets** at 426 kbyte/s, even faster than when we baselined with 10 fast Ethernet ports. 3Com's Corebuilder really picked up speed, moving traffic at an average of 271 kbyte/s per session-nearly twice as fast as its results without congestion and nearly five times faster than it moved **packets** with congestion but

without QOS enabled.

Cabletron, Cisco, and Extreme were all more sluggish with QOS enabled than they were with no QOS and no...

...s results posed a major concern for us: WRED substantially slowed low-priority traffic while only marginally speeding transfers for high-priority packets. Indeed, low- **priority** sessions took more than four times longer to complete with WRED enabled, while high- **priority** sessions moved only 30 percent faster than they did without WRED turned on. Cisco says WRED is doing what it's supposed to. But we noticed that Cisco's switches dropped large amounts of **low - priority** traffic, even after we'd stopped transmitting **high - priority** sessions. We suspect that's because the WRED implementation in the Catalyst 5505 uses only one queue per output port, regardless of priority level. Since we continually kept the queue full, **low - priority** traffic was continually dumped.

Lucent moved **low - priority** sessions the fastest, but the ratio was more like 5:2. Extreme also pushed **low - priority** traffic relatively quickly, but the ratio between **high** - and **low - priority** sessions was more like 2:1 than 4:1.

The Singles Scene

Thus far we've only looked at average forwarding rates. But as we...

...what we found. Cabletron's Smartswitch took an average of 43,000 milliseconds per session to transfer 1 Mbyte of high-priority TCP data with **QOS** enabled. But the difference between the shortest and longest session was nearly 12,000 ms-nearly 30 percent. Extreme's Summit4 also exhibited a variation of 10 percent. The good news is that most switches show less variation in high- **priority** sessions than for other traffic.

Packet traces of individual outbound ports were equally revealing. If a switch comes close to attaining a 4:1 ratio, the natural assumption is that each port would receive four **high - priority** packets, followed by one **low - priority** packet. In other words, we expected to see interleaving at the packet level.

But we saw something more like interleaving at the TCP window level: one window (45 packets) of **high - priority** traffic, followed by 45, 90, or even 135 packets of **low - priority** traffic.

This is a problem for two reasons. It nearly reverses the desired 4:1 ratio, and **high - priority packets** get stuck behind lots of **low - priority** traffic. And that leads to latency; an app could time out in the time it takes to send even one window's worth of **low - priority** traffic.

There's another hidden problem. Everything may look OK on the backbone, where the traffic from 16 outbound ports is flowing together. But pull...real-time voice, video, and multimedia. Jitter-the variation in delay-is also key for voice and video.

We generated two 64-kbyte bursts of **high** -priority POP3 traffic to each of 10 ports in parallel. We also offered five low-priority steady-state Web sessions to the 10 ports. And...

...same amount of time to get through the switch, regardless of priority. Note that all switches except Cisco's significantly increased per-packet latency of **low - priority** traffic when QOS was enabled.

All Shook up

We also measured jitter for **high** - and **low - priority** traffic (see Figure 3). Cisco's switches were far and away the most consistent with QOS enabled, posting variations of just 73 microseconds and 62 microseconds for **high** - and **low - priority** packets. Lucent's 56-microseconds jitter was the lowest we recorded. Cabletron's Smartswitch Router 2000 exhibited more jitter on **high - priority** sessions than low.

One very disturbing result for all vendors except Cisco is that jitter is far higher with QOS enabled. In the case of Extreme's Summit4, for example, jitter for **high - priority** traffic jumps from 10 microseconds to 210 microseconds when QOS is enabled. It's even worse with low -priority traffic; there, jitter jumps from 7 microseconds without QOS to 2,297 microseconds with **QOS** enabled.

To put these results in perspective, even the highest jitter recorded, Cabletron's 4 ms, is still a trifling amount for most apps. But ...link, since we offered traffic from 16 ports through a pipe capable of servicing a maximum of 10. We also designated two classes of traffic, **high**

...low priority, with a different TCP port number assigned to each. We ...ered a total of 27 sessions to each port-nine of high...

...asked vendors to enable their QOS capabilities and ran the same measurements once more, this time noting forwarding rate and variation in session times for **high** - and **low** - **priority** traffic.

In the tests involving bursty traffic, we asked vendors to configure their switches so that **high** - **priority** traffic would receive four times the bandwidth of **low** - **priority** sessions. We then offered each client port a burst of 64 kbytes of **high** - **priority** TCP data, followed by a gap of 300 milliseconds, followed by another 64-kbyte burst. At the same time, we also offered each client port five steady-state streams of **low** - **priority** sessions, each comprising 256 kbytes of TCP data. We measured latency for each packet of all **high** - and **low** - **priority** sessions, and used standard deviation of latency to calculate jitter.

Not all vendors' configurations were identical. Cabletron Systems Inc. (Rochester, N.H.) was unable to...

38/3,K/15 (Item 8 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

...6137809 Supplier Number: 53897699 (USE FORMAT 7 FOR FULLTEXT)
Delivering Quality of Service on the Internet.(Internet/Web/Online Service Information)
...tman, David H.
...ommunications, v33, n2, p35(1)
Feb, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1761

... a single provider.

The DiffServ group defines PHBs that allow IP QoS to scale in service provider backbones and to integrate with pre-existing LAN **QoS** at border routers. IP **QoS** uses the mechanisms developed for ATM **QoS** , while adding some new mechanisms specific to IP It allows service providers to offer new services to their customers, while its ATM heritage simplifies **QoS** interworking in hybrid IP-ATM networks.

Implementation of Differentiated Services Per-Hop Behaviors

PHB	Input Policing Scheduling	Output Management	Congestion
Best Effort	None	**Lowest priority** queuing	Most likely to be dropped
Assured Forwarding	Police on sus- trained and burst	In-Contract: Better- priority queuing	In-Contract: Won't be dropped
...rates. Burst and Burst: Lake-In-Contract Burst: May be dropped			
...re	out-of-contract **packets** Like Best Effort marked.	Out-of-Contract: Like Best Effort	Out-of-Contract:
Expedited Forwarding	Police on sustained rate. Out-of-contract packets are dropped.	**Highest priority** queuing. (Traffic is also shaped.)	Won't be dropped

...

38/3,K/16 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05658772 Supplier Number: 50117590 (USE FORMAT 7 FOR FULLTEXT)
IP TELEPHONY: OPS HANDICAP ITS CHANCES
Multichannel News, v19, n23, p3A
June 8, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Magazine/Journal; Trade
Word Count: 4649

... Yes. Today, you can't assign bandwidth on a per-modem basis. All of the traffic generated in the modem needs to be assigned with **high** or **low priority** . You cannot tier services with today's modems.

Data traffic, for example, will be handled differently than computer-voice traffic. What the **QOS** will allow us to do is to have what we call multiple identified **packets** , by service type. Via that identification, we can tell the system that this **packet** is a voice **packet** , and I need a **high priority** , versus a data **packet** that may have a **lower priority** . It will allow us to do **packet** classifications, so that we could do constant bit rate, or have just best-effort traffic in there.

One of the other components with voice that is unique is that it is also very sensitive to jitter. So not only do we have to transfer the **packet** within a time frame, but the variations of timing between packets have to be constant, so that the system can understand it.

Most of this...

38/3,K/17 (Item 10 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05610630 Supplier Number: 48489089 (USE FORMAT 7 FOR FULLTEXT)
Ready, set, Go
Armitage, Vikram Karmarkar; Grenville
Telephony, pN/A
May 18, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2037

... security and perhaps even offering some firewall protection.

Data in a class by itself A routing system must perform three basic tasks to deliver differentiated **QOS** levels: classification, queuing and scheduling. Classification must happen first so that **packets** with **high priority** aren't stashed temporarily behind **lower - priority** ones. Queuing keeps groups of **packets** belonging to the same message or the same flow together. And scheduling ensures that each customer and its internal groups get the guaranteed bandwidth, that...

38/3,K/18 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05589260 Supplier Number: 48460991 (USE FORMAT 7 FOR FULLTEXT)
Is Layer 4 Switching Technology For Real?
Higgins, Kelly Jackson
Network Computing, p30
May 1, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1227

... to address this issue of burst management."

So what's the real difference between Alteon's flavor of Layer 4 and Yago's Layer 4 **QoS** ? Lo says it's that Yago's MSR switch line doesn't

manage the **packet** sessions; it merely determines whether to peg the traffic as **high** or **low** **priority** . "It doesn't map each session to a particular connection, so it cannot do server load-balancing or firewalling by sessions," according to Lo.

For...

38/3,K/19 (Item 12 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05360457 Supplier Number: 48153101 (USE FORMAT 7 FOR FULLTEXT)
Internet Protocol choice: Sonet or ATM?
Gupta, Rajeev
Electronic Engineering Times, p100
Dec 1, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1409

... bandwidth for each stream.

IP over Sonet requires PPP, which does not have any provision for bandwidth management. The IP Layer has to schedule its **packet** transmissions to ensure that each information flow receives its fair share of link bandwidth. IP-level **packet** scheduling presents problems for slow links, in which the transmission of a large **packet** belonging to a **low** - **priority** flow, such as a file-transfer block, can stall the transmission of a **high** - **priority** flow, such as a voice **packet** . For example, in the future wide-area corporate intranets will most likely run their telephone networks over the same channels as their data networks. The...

...essential as voice transmission requires a constant stream that cannot be blocked by data traffic in tight bandwidth situations.

ATM provides a rich set of **Quality** of **Service** parameters, as well as intelligent queuing and scheduling mechanisms in the switches, to ensure negotiated QoS. On the other hand, PPP does not provide any...

38/3,K/20 (Item 13 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05048931 Supplier Number: 47411625 (USE FORMAT 7 FOR FULLTEXT)
Networking ICs Mmc ships five-piece solution -- Chip set gives Quality-of-Service levels to IP traffic
Wirbel, Loring
Electronic Engineering Times, p58
May 26, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 693

... as Ipsilon Flow Mapping Protocol or Cisco Systems Inc.'s tag-switching protocol. Kennedy said that class-of-service standards typically two simple classes of **high** and **low** - **priority** traffic, but do not spell out how to distribute fairness inside a priority class.

Per-flow queuing answers the problem by abandoning all traditional FIFO architectures, and assigning all IP **packet** flows to separate queues. Queues get assigned to class-of-service groups of queues, and each of the queue group is assigned a weight. Flows that exceed **QoS** thresholds are tagged, and designers can implement their own policing algorithms to control the traffic, though MMC also will implement different traffic policing methods.

MMC...

38/3,K/21 (Item 14 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04501270 Supplier Number: 46610879
Start-up 'autosenses' switching opportunity.
Network World, p1
August 6, 1996
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
...costs between $300 and $400 per port. A NetICs official states that the switches are multimedia-ready. The switches also have a feature called Priority **Quality** of **Service** (PQoS). This feature, which enables the switches to give priority to latency-sensitive **packets** , allows users to define **packets** as **high** -or **low - priority** by media access control (MAC) address, conversion pairs, or by the 3Com Corp. technology, Priority Access Control Enabled (PACE). The PQoS switches can be used...

38/3,K/22 **(Item 1 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

[illegible]-44 SUPPLIER NUMBER: 54935162 (USE FORMAT 7 OR 9 FOR FULL TEXT)
SWITCHING & TRANSMISSION; Surviving the packet revolution.(development of packetized networks for 21st century)(Technology Information)
Telephony, NA
June 7, 1999
ISSN: 0040-2656 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1751 LINE COUNT: 00144

... has strict latency requirements. In a mixed voice and data packet network, the key challenge is to ensure low latency for voice while handling data **packets** as efficiently as possible. In other words, carriers shouldn't penalize the data by carrying voice or degrade voice quality by carrying data. A number...

...be adopted to optimize this balance:
- Packet prioritization. A service provider can assign a priority to an individual packet by manipulating a label in the **packet** header. **Higher - priority packets** gain the right to "bump" **lower priority packets** in order to get to the top of the queue. Significant work is underway to bring guaranteed QOS to **packet** networks, specific schemes include multiprotocol label switching. Applying the **highest priority** to voice **packets** ensures that these **packets** receive the **highest priority** from the network element resources.
- Latency management. Larger **packets** take more time to process onto [illegible] links than smaller **packets** . No matter what size it is, once a [illegible] has been passed from the queue to the link, it's gone. If this were ...

38/3,K/23 **(Item 2 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10511843 SUPPLIER NUMBER: 21192412 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Jerky Video Be Gone: QoS For Ethernet Is Here.(Gigabit Ethernet switch manufacturers are beginning to support the 802.1q standard for quality of service, allowing high-priority traffic to get preference over other traffic) (Technology Information)(Column)
Rash, Wayne
InternetWeek, n735, p66(1)
Oct 5, 1998
DOCUMENT TYPE: Column ISSN: 1096-9969 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 824 LINE COUNT: 00065

... video feed, and until recently, Ethernet did not.

Now that's changed. Gigabit Ethernet switch manufacturers are beginning to support the 802.1q standard for **QoS** , which, if it works right, should ensure that **high - priority** traffic gets preference over other traffic.

The ability to define **high - priority** traffic is important on a busy network. Should a portion of the backbone become oversubscribed, the switches on that segment should discard **low - priority** data **packets** while ensuring that the **higher - priority** traffic passes along the network unscathed.

One of the objects of our testing is to ensure that the goals of **QoS** are actually met. To do this, we used an MPEG-2 codec from Optivision on each end of our backbone, and used the devices to...

38/3,K/24 **(Item 3 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10371069 SUPPLIER NUMBER: 20900074 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Ready, set, go. (routers)
Karmarkar, Vikram; Armitage, Grenville
Telephony, v234, n20, p98(4)
May 18, 1998
ISSN: 0040-2656 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2244 LINE COUNT: 00179

... security and perhaps even offering some firewall protection.

Data in a class by itself

A routing system must perform three basic tasks to deliver differentiated **QOS** levels: classification, queuing and scheduling. Classification must happen first so that **packets** with **high priority** aren't stashed temporarily behind **lower - priority** ones. Queuing keeps groups of **packets** belonging to the same message or the same flow together. And scheduling ensures that each customer and its internal groups get the guaranteed bandwidth, that...

38/3,K/25 **(Item 4 from file: 148)**
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

02340079 SUPPLIER NUMBER: 17878860 (USE FORMAT 7 OR 9 FOR FULL TEXT)
TCP/IP congestion control: can you win the battle? (Transmission Control Protocol/Internet Protocol)
Waclawsky, John G.
Business Communications Review, v25, n11, p75(3)
Nov, 1995
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2374 LINE COUNT: 00206

... go to the same address.

The bottom line is that the guesswork employed in these prioritization schemes doesn't solve the basic problem: getting acknowledgment **packets** back to the sender without delay. Moreover, their focus on **high - priority** traffic throughput necessarily neglects the so-called **low - priority** traffic. Yet when **low - priority** traffic is delayed sufficiently, its senders will also retransmit, further increasing network load and potentially causing timeouts or a congestion collapse.

Since connectionless environments can't provide preferential treatment for acknowledgments, how can they provide adequate prioritization for other kinds of traffic (e.g., **Quality** of **Service**)? This is one of the issues that drove ATM to adopt a connection-based network. Meanwhile, prioritization in connectionless environments remains an open research problem...

38/3,K/26 **(Item 1 from file: 15)**

DIALOG(R)File 15:ABI/Inform(R)

01952325 46243123
Caught up on video
Fritz, Jeffrey
Data Communications v28n15 PP: 51-55 Oct 21, 1999
ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 2704

...TEXT: services as Diffserv (differentiated services), IP precedence, MPLS (multiprotocol label switching), RSVP (resource reservation protocol), and 802. 1p are helping improve things on the IP **QOS** front (seeTable 2).

QOS , CONTINUED

To process different priority levels, a switch or router must be constructed with multiple queues for every port. Queues are like holding tanks for the various priority levels, and when there's more than one, **higher - priority packets** can be prioritized and moved ahead of traffic assigned a **lower priority** level.

Unfortunately, many switches and routers have single queues only. When there's congestion, all **packets** begin lining up in the same queue-which isn't good as far as video is concerned. So try to upgrade switches and routers so...

38/3,K/27 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01836751 04-87742
Surviving the packet revolution
Noblet, Brad
Telephony v236n23 PP: 130-134 Jun 7, 1999
ISSN: 0040-2656 JRNL CODE: TPH
WORD COUNT: 1687

...TEXT: has strict latency requirements. In a mixed voice and data packet network, the key challenge is to ensure low latency for voice while handling data **packets** as efficiently as possible. In other words, carriers shouldn't penalize the data by carrying voice or degrade voice quality by carrying data. A number...

...Illustration Omitted)

Captioned as: FIGURE 2

Packet prioritization. A service provider can assign a priority to an individual packet by manipulating a label in the **packet** header. **Higher -- priority packets** gain the right to "bump" **lower priority packets** in order to get to the top of the queue. Significant work is underway to bring guaranteed QOS to **packet** networks, specific schemes include multiprotocol label switching. Applying the **highest priority** to voice **packets** ensures that these **packets** receive the **highest priority** from the network element resources.

Latency management. Larger **packets** take more time to process onto physical links than smaller **packets** . No matter what size it is, once a packet has been passed from the queue to the link, it's gone. If this were a...

38/3,K/28 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01823597 04-74588
Empowering policy
Mandeville, Robert; Newman, David
Data Communications v28n7 PP: 60-72 May 1999
ISSN: 0363-6399 JRNL CODE: DCM
WORD COUNT: 4474

...TEXT: to control TCP. Several vendors told us our capabilities were more advanced than their internal testing mechanisms and gave them a deeper understanding of how **QOS** works.

TIME AND PUNISHMENT

We conducted four sets of tests. First, we offered steady-state traffic and took baseline measurements of forwarding rate with no...

...Cabletron and Cisco), destined for the same number of ports on the other side of the backbone link. Nine of these 27 sessions transferred high- **priority** POP3 (post office protocol version 3) data over TCP port 110; the balance were low- **priority** HTTP sessions using TCP port 80. Both **highand low - priority** sessions transferred 1 Mbyte of TCP data over the backbone.

Because traffic from 10 fast Ethernet ports is theoretically capable of being carried by a...Ethernet backbone.

To find out if QOS can help, we headed back to the test bed. This time we asked vendors to enable QOS so **high - priority** traffic would receive four times the bandwidth of **low priority** . Then we offered the switches the same load as in the prior round: nine highpriority and 18 **low - priority** TCP sessions to each of 16 inbound ports.

We were mainly interested in determining if forwarding rates for highpriority traffic improve with QOS enabled. We also were curious to see what would happen to **low - priority** trafficwould switches deliver a 4:1 ratio?

Activating QOS made a difference for all switches-but there were big variations. Lucent's Cajun pushed **high** -priority **packets** at 426 kbyte/s, even faster than when we baselined with 10 fast Ethernet ports. 3Com's Corebuilder really picked up speed, moving traffic at an average of 271 kbyte/s per session-nearly twice as fast as its results without congestion and nearly five times faster than it moved **packets** with congestion but without QOS enabled.

Cabletron, Cisco, and Extreme were all more sluggish with QOS enabled than they were with no QOS and no...

... Cisco's results posed a major concern for us: WRED substantially slowed low-priority traffic while only marginally speeding transfers for highpriority packets. Indeed, low- **priority** sessions took more than four times longer to complete with WRED enabled, while high- **priority** sessions moved only 30 percent faster than they did without WRED turned on. Cisco says WRED is doing what it's supposed to. But we noticed that Cisco's switches dropped large amounts of **low - priority** traffic, even after we'd stopped transmitting **high - priority** sessions. We suspect that's because the WRED implementation in the Catalyst 5505 uses only one queue per output port, regardless of priority level. Since we continually kept the queue full, **low - priority** traffic was continually dumped.

Lucent moved **low - priority** sessions the fastest, but the ratio was more like 5:2. Extreme also pushed **low - priority** traffic relatively quickly, but the ratio between **high** - and **low - priority** sessions was more like 2:1 than 4:1.
THE SINGLES SCENE

Thus far we've only looked at average forwarding rates. But as we...

... what we found. Cabletron's Smartswitch took an average of 43,000 milliseconds per session to transfer 1 Mbyte of high-priority TCP data with QOS enabled. But the difference between the shortest and longest session was nearly 12,000 msnearly 30 percent. Extreme's Summit4 also exhibited a variation of 10 percent. The good news is that most switches show less variation in high- priority sessions than for other traffic.

Packet traces of individual outbound ports were equally revealing. If a switch comes close to attaining a 4:1 ratio, the natural assumption is that each port would receive four high - priority packets, followed by one low - priority packet. In other words, we expected to see interleaving at the packet level.

But we saw something more like interleaving at the TCP window level: one window (45 packets) of high - priority traffic, followed by 45, 90, or even 135 packets of low - priority traffic. This is a problem for two reasons. It nearly reverses the desired 4:1 ratio, and high - priority packets get stuck behind lots of low - priority traffic. And that leads to latency; an app could time out in the time it takes to send even one window's worth of low - priority traffic.

There's another hidden problem. Everything may look OK on the backbone, where the traffic from 16 outbound ports is flowing together. But pull... real-time voice, video, and multimedia. Jitter-the variation in delay-is the key for voice and video. We generated two 64-kbyte bursts of high priority POP3 traffic to each of 10 ports in parallel. We also offered low-priority steady-state Web sessions to the 10 ports. And...

... the same amount of time to get through the switch, regardless of priority. Note that all switches except Cisco's significantly increased perpacket latency of low - priority traffic when QOS was enabled.

ALL SHOOK UP

We also measured jitter for high - and low - priority traffic (see Figure 3). Cisco's switches were far and away the most consistent with QOS enabled, posting variations of just 73 ps and 62 ,us for high - and low - priority packets. Lucent's 56-ps jitter was the lowest we recorded. Cabletron's Smartswitch Router 2000 exhibited more jitter on high - priority sessions than low.
One very disturbing result for all vendors except Cisco is that jitter is far higher with QOS enabled. In the case of Extreme 's Summit4, for example, jitter for high - priority traffic jumps from 10 its to 210 gis when QOS is enabled. It's even worse with low -priority traffic; there, jitter jumps from 7 ps without QOS to 2,297 ps with QOS enabled.

To put these results in perspective, even the highest jitter recorded, Cabletron's 4 ms, is still a trifling amount for most apps. But...link, since we offered traffic from 16 ports through a pipe capable of servicing a maximum of 10. We also designated two classes of traffic, high and low priority, with a different TCP port number assigned to each. We offered a total of 27 sessions to each port-nine of high...

... asked vendors to enable their QOS capabilities and ran the same measurements once more, this time noting forwarding rate and variation in session times for high - and low - priority traffic.

In the tests involving bursty traffic, we asked vendors to configure their switches so that high - priority traffic would receive four times the bandwidth of low - priority sessions. We then offered each client port a burst of 64 kbytes of high - priority TCP data, followed by a gap of 300 milliseconds, followed by another 64-kbyte burst. At the same time, we also offered each client port five steady-state streams of low - priority sessions, each comprising 256 kbytes of TCP data. We measured latency for each packet of all high - and low - priority sessions, and used standard deviation of latency to calculate jitter.

Not all vendors' configurations were identical. Cabletron Systems Inc.

(Rochester, N.H.) was unable to...

38/3,K/29 **(Item 4 from file: 15)**
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01685357 03-36347
Say what?
Hindin, Eric
Network World v15n33 PP: 37-39 Aug 17, 1998
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 2344

...TEXT: to configure their software to ask for the best possible service level. Administrators would probably need to establish rules for users and ... even configure **QoS** on a per-user basis.

... data is prioritized using implicit or explicit techniques, queues and queuing algorithms are used to provide the appropriate or desired **QoS** .

Queues, which are simply areas of memory within a router or switch, are set up to contain different priority **packets** . A queuing algorithm determines the order in which **packets** stored in the queues are transmitted. The idea is to give better service to **high - priority** traffic while ensuring, to varying degrees, that **low - priority** **packets** get some service.
The graphic on page 37 shows basic implicit and explicit **QoS** systems. A queuing algorithm dictates that the queues are serviced on a roundrobin basis. The algorithm specifies the transmission of two **packets** from Queue 1 (the **high - priority** queue) for every one **packet** transmitted from Queues 2 and 3. Same-priority **packets** are transmitted from within each queue on a first in, first out (FIFO) basis.

If congestion occurs, the queuing system does not guarantee crucial data will reach its destination in a timely manner; it only ensures that high-priority **packets** will get there before lowpriority **packets** .

More sophisticated **QoS** systems solve this problem with bandwidth reservation systems, which assign prespecified amounts of bandwidth to individual queues or groups of queues. This ensures that bandwidth is always available for a **high - priority** queue. **QoS** is guaranteed unless the data in a queue exceeds the amount of reserved bandwidth. If this happens, the algorithms usually allow bandwidth from **low - priority** queues to service **high - priority** traffic, and vice-versa.

Basic queuing algorithms transmit **packets** from the same queue in a FIFO order. Large frames associated with a **high - priority** file transfer may delay a transaction processing application that passes small amounts of data, even though **packets** from both applications are classified as **high priority** .

More sophisticated queuing algorithms attempt to be fairer. For example, Cisco's weighted fair queuing (WFQ) differentiates among bandwidth-hogging applications and those that need...

38/3,K/30 **(Item 5 from file: 15)**
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01683848 03-34838
WideBand gigabit networking
Billings, Roger E
Computer Technology Review v18n7 PP: 20-22 Jul 1998
ISSN: 0278-9647 JRNL CODE: CTN
WORD COUNT: 1561

...TEXT: expansion. This feature prevents buffer overflows and retransmission delays.

Class Of Service

WideBand supports a class of service feature similar to that of ATM. Every **packet** loaded onto a WideBand network is assigned a class of service level. Data with a **high priority** is delivered across networking resources before data of a **lower priority** . Utilizing this method, **high priority** data can be delivered in a timely fashion, even on very busy networks, while **low - priority** , time consuming applications, such as batch editing of large databases, can operate at the full network bandwidth available, without interfering with crisp and reliable performance for other, **higher - priority** users.

Quality Of Service

WideBand provides **Quality** of **Service** . Certain types of data require on-time delivery. Video, for example, if not delivered precisely on time, becomes jerky. When interspersing streaming data such as...

38/3,K/31 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01651181 03-02171
Fly my way
Moreland, Chuck; Huang, Alan
Telephony v234n23 PP: 118-122 Jun 8, 1998
ISSN: 0040-2656 JRNL CODE: TPH
WORD COUNT: 1681

...TEXT: starvation when higher-class traffic exceeds the available bandwidth. This problem has the potential to escalate into serious congestion as the source retransmits delayed IP **packets** .

Advanced traffic management avoids bandwidth starvation by allowing a service provider to assign each service class a minimum bandwidth guarantee. This reduces the **QOS** effect on **lower - priority** traffic of the temporary presence of excess **higher - priority** traffic, just as some discount fare seats are available on all flights. A common pool of bandwidth can be set aside and shared on a...

38/3,K/32 (Item 7 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01597975 02-48964
Why you need a QoS scheme
Petrosky, Mary
Network World v15n11 PP: 41 Mar 16, 1998
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 833

...TEXT: control you need to expedite certain types of traffic. For example, with a prioritization scheme in place, you can define SAP R/3 traffic as **high priority** so it will be forwarded before PointCast and other **low - priority** traffic. And if **packets** must be dropped because of congestion, the **low - priority packets** will be dropped first. For organizations that need to control latency, there are more elaborate **QoS** schemes, such as those supported by ATM and the Resource Reservation Protocol (RSVP) . These **QoS** schemes give you control of bandwidth, latency and accuracy levels (meaning which packets get tossed in case of congestion) . RSVP is capable of ensuring that...

38/3,K/33 (Item 8 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01267410 99-16806
Start-up 'autosenses' switching opportunity
Duffy, Jim
Network World v13n32 PP: 1, 13 Aug 5, 1996
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 647

...TEXT: be most unique about the switches-aside from their price- is that they are multimedia-ready, Vacon said. NetICs has developed a feature called Priority **Quality** of **Service** (PQoS) that allows the switches to give priority to latencysensitive **packets** such as voice and video.

With PQoS, users can define **packets** as **high** -or **low** - **priority** based on media access control (MAC) address or conversation pairs, or via 3Com [illegible]'s Priority Access Control Enabled (PACE) technology. PACE lets net [illegible] run real-time voice and video applications over switched 10M and [illegible] Mbit/sec Ethernet links by ensuring delaysensitive traffic gets a higher transmission **priority** .

"We don't think you need cells for multimedia," Vacon said, referring to the common but diminishing belief that ATM is the only way to...

38/3,K/34 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01206945 CMP ACCESSION NUMBER: NWC19991227S0006
Nortel Networks Leads the Pack With Accelar Enterprise Switch
Joel Conover
NETWORK COMPUTING, 1999, n 1026, PG16
PUBLICATION DATE: 991227
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Sneak Previews
WORD COUNT: 1101

... load. Because of Accelar's shared memory architecture, the switch latency remains constant regardless of load or port configuration.

Finally, I tested the switch's **QoS** (**Quality** of **Service**) capabilities. Using two ports to oversubscribe a third, I tested its [illegible] priority queuing mechanism. I offered varying loads of **low** - and **high** - **priority** traffic, and in all cases the Accelar forwarded 100 percent of the **high** - **priority** traffic without any **packet** loss.

I applaud Nortel's decision to include support for eight hardware-based priority queues in the 8600 architecture. The vendor's support for eight classes of service allows for a significant amount of **QoS** granularity in the enterprise backbone.

The icing on the cake for the Accelar 8600 is its aggressive pricing. Nortel has taken huge strides toward making...

38/3,K/35 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01203021 CMP ACCESSION NUMBER: DAC19991021S0018
Caught Up On Video? - Video is about to become a big part of corporate networking. Here's how net architects can prepare for the show
Jeffrey Fritz
DATA COMMUNICATIONS, 1999, n 2815, PG51

PUBLICATION DATE: 991021
JOURNAL CODE: DAC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Feature - Video Apps
WORD COUNT: 2701

... services as Diffserv (differentiated services), IP precedence, MPLS (multiprotocol label switching), RSVP (resource reservation protocol), and 802.1p are helping improve things on the IP **QOS** front (seeTable 2).

QOS , Continued

To process different priority levels, a switch or router must be constructed with multiple queues for every port. Queues are like holding tanks for the various priority levels, and when there's more than one, **higher - priority packets** can be prioritized and moved ahead of traffic assigned a **lower priority** level.

Unfortunately, many switches and routers have single queues only. When there's congestion, all **packets** begin lining up in the same queue -which isn't good as far as video is concerned. So try to upgrade switches and routers so...

38/3,K/36 (Item 3 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01199870 CMP ACCESSION NUMBER: CRN19990913S0028
Lucent delivers DSL with Stinger
Warren S. Hersch
COMPUTER RESELLER NEWS, 1999, n 859, PG26
PUBLICATION DATE: 990913
JOURNAL CODE: CRN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: News
WORD COUNT: 479

... the technology. The offering also is currently in trials at more than 20 customers worldwide.

The product received a mixed reaction from resellers.

"(Stinger's) **QoS** and **packet** prioritization features are what it takes to do voice-over-DSL deployments," said Jeff Carnegie, president of Carnegie Technical Inc., a San Diego-based VAR, adding the product's release was an inevitable step. "But I don't believe any of the routers on the market support **QoS** . And, regarding DSL quality, the router's ability to differentiate between **high - priority** and **low - priority packets** is key," he said.

"This is not a channel product," said Randy Wear, principal of Decisions Systems Plus Inc., a Rosemont, Ill.-based VAR. "An...

38/3,K/37 (Item 4 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01191074 CMP ACCESSION NUMBER: DAC19990507S0022
Empowering Policy - What's the verdict in the industry's first test of Layer 4 switches? Qualified success in adding QOS to TCP apps. But until latency and jitter are brought under control, these boxes can't be considered the cornerstone of the corporate network
Robert Mandeville and David Newman
DATA COMMUNICATIONS, 1999, n 2807, PG60
PUBLICATION DATE: 990507

JOURNAL CODE: DAC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Features - DataComm Lab Test: Layer 4 Switches
WORD COUNT: 4406

... 2000 analyzers from Netcom Systems Inc. (Chatsworth, Calif.) running TCP/IP code developed especially for this test (see "Test Methodology"). The new code timestamps every **packet** it sends and receives with 100- nanosecond accuracy, giving us an unprecedented view of the workings of the QOS mechanisms intended to control TCP. Several...s results posed a major concern for us: WRED substantially slowed low-priority traffic while only marginally speeding transfers for high-priority packets. Indeed, low- **priority** sessions took more than four times longer to complete with WRED enabled, while high- **priority** sessions moved only 30 percent faster than they did without WRED turned on. Cisco says WRED is doing what it's supposed to. But we noticed that Cisco's switches dropped large amounts of **low - priority** traffic, even after we'd stopped transmitting **high - priority** sessions. We suspect that's because the WRED implementation in the Catalyst 5505 uses only one queue per output port, regardless of priority level. Since we continually kept the queue full, **low - priority** traffic was continually dumped.

...moved **low - priority** sessions the fastest, but the ratio was more like 5:2. Extreme also pushed **low - priority** traffic relatively quickly, but the ratio between **high** - and **low - priority** sessions was more like 2:1 than 4:1.

The Singles Scene

Thus far we've only looked at average forwarding rates. But as we... real-time voice, video, and multimedia. Jitter-the variation in delay-is also key for voice and video.

We generated two 64-kbyte bursts of **high** -priority POP3 traffic to each of 10 ports in parallel. We also offered five low-priority steady -state Web sessions to the 10 ports. And...

...same amount of time to get through the switch, regardless of priority. Note that all switches except Cisco's significantly increased per-packet latency of **low - priority** traffic when QOS was enabled.

All Shook up

We also measured jitter for **high** - and **low - priority** traffic (see Figure 3). Cisco's switches were far and away the most consistent with QOS enabled, posting variations of just 73 microseconds and 62 microseconds for **high** - and **low - priority** packets. Lucent's 56-microseconds jitter was the lowest we recorded. Cabletron's Smartswitch Router 2000 exhibited more jitter on **high - priority** sessions than low.

One very disturbing result for all vendors except Cisco is that jitter is far higher with QOS enabled. In the case of Extreme's Summit4, for example, jitter for **high - priority** traffic jumps from 10 microseconds to 210 microseconds when QOS is enabled. It's even worse with **low** -priority traffic; there, jitter jumps from 7 microseconds without QOS to 2,297 microseconds with **QOS** enabled.

To put these results in perspective, even the highest jitter recorded, Cabletron's 4 ms, is still a trifling amount for most apps. But ...link, since we offered traffic from 16 ports through a pipe capable of servicing a maximum of 10. We also designated two classes of traffic, **high** and low priority, with a different TCP port number assigned to each. We offered a total of 27 sessions to each port-nine of high...

...asked vendors to enable their QOS capabilities and ran the same measurements once more, this time noting forwarding rate and variation in session times for **high** - and **low - priority** traffic.

In the tests involving bursty traffic, we asked vendors to configure their switches so that **high - priority** traffic would receive four times the bandwidth of **low - priority** sessions. We then offered each client port a burst of 64 kbytes of **high - priority** TCP data, followed by a gap of 300 milliseconds, followed by another 64-kbyte burst. At the same time, we also offered each client port five steady- state streams of **low - priority** sessions, each comprising 256 kbytes of TCP data. We measured latency for each packet of all **high** - and **low - priority** sessions, and used standard deviation of latency to calculate jitter.

Not all vendors' configurations were identical. Cabletron Systems Inc. (Rochester, N.H.) was unable to...

38/3,K/38 **(Item 5 from file: 647)**
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01174510 CMP ACCESSION NUMBER: INW19981005S0063
Jerky Video Be Gone: QoS For Ethernet Is Here (Rash's Judgment)
Wayne Rash
INTERNETWEEK, 1998, n 735, PG66
PUBLICATION DATE: 981005
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: ...Yada, Yada, Yada...
WORD COUNT: 768

... video feed, and until recently, Ethernet did not.

Now that's changed. Gigabit Ethernet switch manufacturers are beginning to support the 802.1q standard for **QoS** , which, if it works right, should ensure that **high - priority** traffic gets preference over other traffic.

The ability to define **high - priority** traffic is important on a busy network. Should a portion of the backbone become oversubscribed, the switches on that segment should discard **low - priority** data **packets** while ensuring that the **higher - priority** traffic passes along the network unscathed.

One of the objects of our testing is to ensure that the goals of **QoS** are actually met. To do this, we used an MPEG-2 codec from Optivision on each end of our backbone, and used the devices to...

38/3,K/39 (Item 6 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01160695 CMP ACCESSION NUMBER: NWC19980501S0009
Is Layer 4 Switching Technology For Real? (In-depth news analysis)
Kelly Jackson Higgins
NETWORK COMPUTING, 1998, n 908, PG30
PUBLICATION DATE: 980501
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Business Trends
WORD COUNT: 1237

... to address this issue of burst management."

So what's the real difference between Alteon's flavor of Layer 4 and Yago's Layer 4 **QoS** ? Lo says it's that Yago's MSR switch line doesn't manage the **packet** sessions; it merely determines whether to peg the traffic as **high** or **low priority** . "It doesn't map each session to a particular connection, so it cannot do server load-balancing or

firewalling by sessions," according to Lo.

For...

38/3,K/40 (Item 7 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01141961 CMP ACCESSION NUMBER: EET19971020S0100
L4: straightforward path to scalable processing on virtual servers
Selina Lo, Vice President of Marketing, Alteon Networks Inc., San Jose, Calif.
ELECTRONIC ENGINEERING TIMES, 1997, n 976, PG84
PUBLICATION DATE: 971020
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Communications Design
WORD COUNT: 753

... to as Layer 4 switching is the assignment of Quality of Service or Class of Service (QoS or CoS) to a particular application so that **packets** for the application can be queued according to the user-designated application priority. Once queued, these **packets** are still forwarded to the destination port based on the destination L2 or L3 address in the **packet** headers.
In general, enforcing **QoS** or CoS can require a complex set of rules involving many different criteria, such as source and destination addresses (L2 and L3), the application type...
...frames that originate from a server IP address designated for another server IP address can be classified as "server-to-server" traffic and assigned a **lower priority** than client-to-server traffic. Or interactive applications like HTTP might be assigned a **higher priority** than bulk file transfer. Or a video application might include an explicit priority for every frame, giving MPEG I frames a **higher priority** than B or P frames, because their loss would have a more damaging effect on the video stream.
Supporting flexible **QoS** on a switch requires consideration in terms of the number of bytes within each packet the switch must examine to determine a criterion match, and...

38/3,K/41 (Item 8 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01127164 CMP ACCESSION NUMBER: EET19970526S0063
Networking ICs Mmc ships five-piece solution - Chip set gives Quality-of-Service levels to IP traffic
Loring Wirbel
ELECTRONIC ENGINEERING TIMES, 1997, n 955, PG58
PUBLICATION DATE: 970526
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Design
WORD COUNT: 695

... as Ipsilon Flow Mapping Protocol or Cisco Systems Inc.'s tag-switching protocol. Kennedy said that class- of-service standards specify two simple classes of **high** - and **low** - **priority** traffic, but do not set out how to distribute fairness inside a priority class.
Per-flow queuing answers the problem by abandoning all traditional FIFO architectures, and assigning all IP **packet** flows to separate queues. Queues get assigned to class-of-service groups of queues, and each of the queue group is assigned a weight. Flows that exceed **QoS** thresholds are tagged, and designers can implement their own policing algorithms to control the traffic, though MMC also will implement different traffic policing methods.

MMC...

38/3,K/42 **(Item 9 from file: 647)**
DIALOG(R)File 647:CMP Computer Fulltext

01017575 CMP ACCESSION NUMBER: CWK19940704S0667
GOOD REASONS FOR NT DELAY? (Letters to the Editor)
COMMUNICATIONSWEEK, 1994, n 512, 39
PUBLICATION DATE: 940704
JOURNAL CODE: CWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Opinion
WORD COUNT: 1001

... to be clarified.

The ATM Forum standards allow for negotiation of a traffic contract ... a call setup. There are at least two types of **quality** of **service** ... ined. Knowing these, it is very difficult to price **low** - and **high** - **priority** traffic at the same rate; moreover, when TCP/IP traffic like File Transfer Protocol traffic is going over ATM, a loss of a single cell in a frame could cause a retransmission of long **packets** . In this case, the user will of course not pay for the retransmission. Yet, the carrier thinks that there was only one cell lost. As...